2012

Online onslaught: internet-based methods for attacking and defending citizens' organisations

Brian Martin
University of Wollongong, bmartin@uow.edu.au

Publication Details

Martin, B. 2012, 'Online onslaught: internet-based methods for attacking and defending citizens' organisations', First Monday, vol. 17, no. 12, pp. 1-9.

First Monday, Volume 17, Number 12 - 3 December 2012

PEER-REVIEWED JOURNAL ON THE INTERNET

Online onslaught: Internet-based methods for attacking and defending citizens' organisations

by Brian Martin

Abstract

As the online profiles of organisations become more important, so do their vulnerabilities to online attack. A wide range of online methods can be used to attack the credibility of an organisation, deter participation by its members and undermine its operations. A case study from the Australian vaccination debate is used to illustrate the operation and impact of some of these possible methods. The main modes of attack are disrupting discussions, dominating descriptions and ridiculing and intimidating opponents. The main modes of defence are excluding disrupters, providing counter–descriptions, making formal complaints, and ignoring or exposing abuse. New forms of social media in the future will offer additional options for both offence and defence.

Contents

Introduction

It has become commonplace for organisations to have an online presence, for example e–mail lists, Web sites, blogs and Facebook pages. Most such operations are routine, with online activities proceeding with no special difficulties. However, in a small proportion of cases, the online presence of an organisation can become a site of struggle, with opponents — sometimes from the outside, sometimes inside — seeking to control, disrupt or destroy the organisation's online activities.

How can the methods used in such online struggles be understood? There seems to be no standard framework in use. One approach would be to look at military strategy, for example at Karl von Clausewitz's (1832–1834) classic concept of the centre of gravity, Mao Tse–Tung's (1961–1965) ideas on people's war or theories of nuclear deterrence (Kahn, 1961). However, military strategy seems too removed from the online realm, except in the most general sense, to provide much guidance, largely because militaries can legitimately use force against opponents during warfare, whereas no physical force is involved in cyber struggles and actions are subject to laws and regulations.

Another approach is to look at methods of non–violent action, defined as unarmed methods of struggle that go beyond conventional politics, thereby excluding techniques such as lobbying and voting. Gene Sharp (1973), the pioneer researcher in this field, classifies non–violent action into three principal types: (1) protest and persuasion, including petitions and rallies; (2) non–cooperation, including many types of strikes and boycotts; and, (3) intervention, including sit–ins, fasts, sabotage and setting up parallel government. However, Sharp's work was done long before the rise of the Internet, and thus does not include any online methods. Furthermore, Sharp's contrast between violent and nonviolent methods breaks down online, because direct physical harm to others is seldom possible. Furthermore, the concepts of non–

violent action are oriented to activists and communities resisting a powerful, often violent aggressor or oppressor, typically a government or military. No one yet has developed a classification and documentation of online methods of action that might parallel classifications of armed and non–violent struggle (For a promising start, see Digital Activism Research Project [2012].).

There is a large amount of research on cyberwarfare, which includes disrupting enemy digital processes and protecting their own (Carr, 2012; Janczewski and Colarik, 2008; Rattray, 2001). However, many of the methods used, such as viruses and Trojan horses, are considered illegitimate or illegal in civilian life, and hence are unlikely to play a prominent role in an online struggle between public organisations.

Another relevant body of writing is on cyberactivism (Jordan, 2002; McCaughey and Ayers, 2003; Reporters Without Borders, 2005; van de Donk, *et al.*, 2004), which includes using online tools to supplement conventional campaigning — for example to help organise rallies using social media — and as a direct form of activism, such as online petitions. The methods used in cyberactivism (Megens and Martin, 2003) are very relevant, but are oriented to campaigning on social issues, not to inter–organisational struggles.

Cyberbullying (Patchin and Hinduja, 2012) involves harassing individuals using online methods, and is the online manifestation of the long–standing phenomenon of bullying. Most studies of cyberbullying focus on young people as perpetrators and targets, but as with bullying at work, cyberbullying can involve adults. A related type of Internet–based attack is "Internet vigilantism". Common targets include scammers, paedophiles, ID thieves and people who hurt animals.

Both cyberbullying and Internet vigilantism focus on attacks on individuals rather than on entire organisations. Online attacks intended to destroy an organisation could be considered a new type of Internet vigilantism or cyberbullying.

This paper initiates an exploration of methods of inter–organisational cyber–struggle. Unlike cyberactivism and non–violent action, in which groups with less formal and coercive power challenge those with more (for example when protesters challenge authoritarian governments), the focus here is on methods used by online campaigners on both sides of an inter–organisational contest. The methods used by the attackers have affinities with cyberbullying and Internet vigilantism, with the difference that the target has the resources and vulnerabilities of an organisation, not just an individual.

Struggles routinely involve methods of both attack and defence; the approach here is one way into an examination of online methods. Rather than try to build an appropriate framework drawing on prior military, activist or bullying repertoires, the approach here starts with an actual struggle, examining the methods used and proposing categories to put them in, in the spirit of grounded theory (Glaser and Strauss, 1967), in which an immersion in the data is the basis for developing a theoretical framework. Given that there are many possible online struggles to examine, this is necessarily a preliminary step in a process of developing a useful framework.

The next section describes a conflict between two groups involved in the Australian vaccination debate in which online methods have played a prominent role. This case study illustrates several methods of online attack and possible methods of defence or counterattack. In the following section, I use this case study to motivate a classification of methods of online attack and defence, noting the advantages and disadvantages of each. The conclusion outlines the implications of this analysis.

Online methods in an Australian vaccination struggle

Vaccination against infectious diseases is supported by medical professions worldwide (Andre, *et al.*, 2008; Offit and Bell, 2003), and in most countries there is a standard set of vaccinations given to children. In the face of this medical orthodoxy, a small number of citizens' groups and professionals present a contrary position, arguing that the benefits of vaccination have been overestimated and that there are significant risks to individuals and society, with recorded cases of seriously affected children (Habakus and Holland, 2011; Halvorsen, 2007). These can be called vaccine–critical groups (Hobson–West, 2007).

The issue of vaccination can generate great emotions. Both sides invoke children's health, proponents saying that vaccination is an essential defence against deadly childhood diseases such as measles and whooping cough, and critics claiming that many children suffer adverse reactions to vaccines. For the following discussion of online tactics, it is not necessary to know details of the arguments for and against vaccination. What is important is to know that each side contains many individuals highly committed to their beliefs.

The Australian Vaccination Network (AVN) is a typical vaccine–critical group. Established in 1994, it presents itself as pro–choice, arguing that parents should be informed of arguments on both sides before vaccinating their children. The AVN is a citizens' group, without backing from any other organisation. Its founder and key figure is Meryl Dorey, a mother and self–taught advocate. The AVN is an incorporated body with a constitution and an elected committee.

In 2009, another group was formed: Stop the Australian Vaccination Network (SAVN). Its avowed purpose is to shut down the AVN. SAVN, like the AVN, is a citizen–based group, with

some links to the Australian Skeptics. Some of those involved in SAVN are doctors, nurses or science students, but SAVN has no overt ties to professional medical associations. SAVN's only presence is online. It is not incorporated, and apparently has no bank account or any physical office. It does not have formal members, but rather Facebook friends. For convenience, participants in SAVN's activities are called here SAVNers.

The AVN and SAVN have been engaged in an ongoing struggle, with SAVN trying to bring down the AVN and the AVN trying to survive the attack and continue its activities. In this struggle, various techniques have been used. It is not straightforward to classify SAVN's attack methods as entirely online or off–line. For convenience, it is useful to distinguish methods that target the AVN's off–line activities from those that target the AVN's online presence. Methods targeting the AVN's off–line activities include:

- Complaints to state government regulatory bodies, such as the Health Care Complaints Commission, the Office of Liquor, Gaming and Racing (which regulates charitable status) and the Department of Fair Trading, all of which deal with organisations incorporated in the state of New South Wales
- Letters to organisations, such as libraries, hosting talks by Dorey, with the aim of stopping the talks;
- Letters to commercial bodies selling the AVN's magazine *Living Wisdom*, with the aim of blocking sales
- Advertisements attacking the AVN placed in local newspapers in regions where Dorey was giving a talk
- Hiring of a plane to fly a banner saying "Vaccination saves lives" over a folk festival venue where Dorey was giving a talk

Some of the complaints and letters are made off–line, using the telephone or post; others are communicated online, using e–mail. However, my focus here is on techniques that target the AVN's online presence.

Some members of the AVN, in responding to SAVN attacks, have occasionally used some of the same sorts of techniques as SAVN, for example making hostile comments on SAVN's page. Overall, though, in this confrontation SAVN has predominantly taken an attacking role and AVN members have mainly been defenders.

The rationales given by SAVN attackers vary. Some argue that in Australia there is no constitutional protection of free speech, so speech by AVN members is not guaranteed. Others say that they support free speech, but not AVN speech because it is false and dangerous. Still others defend their actions by referring to their own freedom of speech to present damaging material about the AVN in various forums. However, for the purposes of examining online tactics, the rationales for the attack and defence are not central, so a detailed assessment of SAVN justifications for actions taken, or of AVN arguments in its defence, is not needed.

Web addresses

AVN (Australian Vaccination Network)
Web site, http://www.avn.org.au/
Facebook,
http://www.facebook.com/home.php#!/avn.living.wisdom

SAVN (Stop the Australian Vaccination Network)
Facebook, http://www.facebook.com/stopavn

VAIS (Vaccination Awareness and Information Service)
Web site, http://www.antivaxxers.com/
Hall of Shame, http://www.antivaxxers.com/?p=3792

Web of Trust
Web site, http://www.mywot.com/
Rating of AVN,
http://www.mywot.com/en/scorecard/www.avn.org.au

Seven methods used to attack the AVN are described here. This is not an exhaustive list, but does give a sense of the variety of methods of attack and defence in this case that could well be used in other struggles.

Attack method 1: Make contrary comments on the target's blog

SAVNers have made comments on the AVN's blog. This seems innocuous, except that from an AVN point of view, it turns a discussion among sympathisers about issues of concern into a contentious disputation of ideas. Furthermore, some of the SAVN comments have been abusive, for example calling Dorey a liar and hypocrite. The AVN has several possible responses.

1. Accept all SAVN comments and allow them to be addressed by AVN members. This might be feasible if SAVN comments were a small minority of total comments. However, SAVN has some very energetic correspondents who, if given the opportunity, would virtually monopolise the AVN blog. Therefore, this option would mean relinquishing the

AVN blog to its opponents.

2. Accept only polite SAVN comments. This only partially solves the problem that the AVN blog could be taken over — especially when many AVN members are afraid to contribute (see below).

3. Make the blog invisible to non–members. This would prevent most SAVN comments, but at the expense of hiding the blog from potentially interested members of the public.

4. Delete or block comments contrary to the AVN's general orientation and, on Facebook, bar those who make them. This prevents SAVN friends from contributing under their own names or under false identities. However, it is open to the charge of censorship.

5. Set up a moderated group for "respectful comments about vaccination" as an outlet for SAVN and other critics.

The AVN initially used options 1 and 2 but over time shifted to 4 and 5.

Attack method 2: Ridicule screenshots from the target's page

SAVNers follow the AVN's blog and Web site, take screenshots of selected commentary, post the screenshots on SAVN's Facebook page and condemn or ridicule the comments and/or the authors. For example, in one case, a screenshot was accompanied by reference to the author as "repugnant," "vicious" and "contemptible."

This sort of treatment can be distressing to some AVN contributors, who unexpectedly find their comments about vaccination the target of sarcasm, humour or abusive comment. Sometimes, SAVNers target an individual, searching for any online comments by the person, posting selected portions of the comments and holding them up to ridicule. This technique has discouraged some AVN members from making any online comment.

One possible response by AVN members would be to make posts under false identities. This has the disadvantage of reducing the authenticity of contributions; if widely followed, it would become harder to trust anyone's comments.

In 2011, the AVN complained to Facebook about SAVN's page, which apparently violates Facebook policy about not attacking others. SAVN then restricted the visibility of its wall and photos to members and set up another open page. Some months later, SAVN opened its original page for general viewing. The AVN's complaint to Facebook thus did not overcome the problem of SAVN's screenshot–posting tactic.

Attack method 3: Track and adversely comment on target members' blog comments

As well as making long comments on the AVN's blog, Meryl Dorey regularly comments on blogs elsewhere. Sometimes, when SAVNers find out about her blog comments, they add their own comments.

For example, a member of a U.S. vaccine–critical group posted on the group's blog a photo of a billboard saying "No shots, no school ... not true!!!" (Piper–Terry, 2011). Other members of the group made complimentary comments — and then Dorey added her own supportive comment. Shortly after, SAVNers posted comments questioning and challenging the beliefs of the vaccine–critical group, for example suggesting that their children's disabilities might not have been due to vaccines. The blog was thus transformed from an in-house discussion to a confrontation with pro–vaccinationists.

Dorey assumed that SAVNers had set up a Google Alert for her name and thus were notified about any blog comment she made anywhere on the Internet. One response she could make is to notify blog moderators as soon as SAVN interventions occur, so SAVN interveners could be blocked and their comments deleted, if desired. Another response she could make is to use a pseudonym, even a slight variation on her name.

There is nothing illegal about putting a Google Alert on someone's name and then attempting to post damaging information about the person any time the person in question makes a comment. However, many targets would find this confronting and distressing.

Attack method 4: Monopolise Wikipedia entries

There is an extensive Wikipedia entry on the AVN, much lengthier than for most organisations of similar size and influence. For example, the Wikipedia entry for Whistleblowers Australia, which has a public profile roughly similar to the AVN's, is quite brief and incomplete. The entry on the AVN conforms to Wikipedia expectations in form. A close reading indicates that it almost certainly has been written by opponents of AVN. For example, there is extensive reference to a warning about the AVN from the Health Care Complaints Commission. There is also a Wikipedia entry for SAVN.

When opponents take over a Wikipedia entry, one avenue for resistance is counter–editing. Indeed, Wikipedia depends for its accuracy on vigorous engagement in contentious areas. However, SAVNers seem to have the numbers, energy and resources sufficient to overwhelm any attempt by AVN supporters to modify the entry. Another option, seemingly adopted by AVN members, is simply to ignore the Wikipedia entry and to concentrate energies on the online forums it can control, especially its own Web pages.

Attack method 5: Make adverse comments on Side Wikis

A Side Wiki is a place for comments on a Web page, visible to anyone visiting the page by using Google Side Wiki software. SAVNers have made critical comments about the AVN on the

Side Wiki for the AVN's Web page.

One possible response from AVN members would be to add their own Side Wiki comments. Another is simply to ignore the Side Wikis, because not that many people take any notice of them, which seems to have been the primary AVN response. In retrospect this was a sensible option, given that Google discontinued Side Wikis in 2011.

Attack method 6: Send adverse ratings to the Web of Trust

The Web of Trust is a system for rating Web sites. Anyone can log into the Web of Trust site and give a rating to any site, essentially either to trust it or not to trust it. The primary purpose of the Web of Trust, it seems, is to provide guidance for parents about sites suitable for their children, for example about pornographic sites. When subscribers to the Web of Trust access sites that have received a sufficient proportion of adverse reports, the sites come on the screen accompanied by a warning message.

Opponents of the AVN contacted the Web of Trust and made numerous adverse ratings and comments about the AVN's Web site. As a result, putting the AVN's Web address into the Web of Trust generates a notice: "Warning! This site has a poor reputation."

Facebook subscribes to the Web of Trust, and prevents anyone putting a link to a site with an adverse Web–of–Trust rating. This means that the AVN is not allowed to put a link from its Facebook page to its own Web site, a significant restriction when sending notices to Facebook friends.

The AVN could simply ignore the adverse Web–of–Trust ratings on the grounds that not many people subscribe to the Web of Trust. To challenge the adverse rating, the AVN could encourage members to put in positive ratings of the AVN's site, though it is hard to know how many are necessary: the Web of Trust does not reveal its algorithm for combining individual ratings into an overall rating. Another option is to complain to the Web of Trust about an orchestrated campaign by SAVN and to complain to Facebook about its uncritical use of the Web of Trust ratings. Yet another option is to switch from Facebook to another platform such as Google+.

In practice, the AVN made complaints to both the Web of Trust and Facebook, to no avail, so its de-facto stance has been to ignore the Web of Trust's adverse rating. Another possible AVN response would be to include on its own Web site an explanation of the way its Web–of–Trust rating has been manipulated. However, this might have the effect of alerting more people to the Web of Trust, not a useful tactic if visitors have never heard of it.

Attack method 7: Set up a Hall of Shame

The Vaccination Awareness and Information Service (VAIS) is, like SAVN, an opponent of the AVN. VAIS set up a "Hall of Shame" listing the names and addresses of dozens of chiropractors, natural health practitioners and others who have advertised in the AVN's magazine *Living Wisdom*. The Hall of Shame is an attempt to stigmatise the individuals and enterprises named; it also opens them to harassment from supporters of vaccination. Some of those listed in the Hall of Shame might feel threatened by the public display of their contact details in this context, and prefer to withdraw their advertisements. For issue number 8 of *Living Wisdom* published in 2011, Dorey did not accept any new ads (running only a few prepaid ones) because she did not want to open individuals or businesses to harassment.

Offence and defence

The various online methods used against the AVN can be grouped into ideal types, namely characteristic approaches to offence. To understand these types, it is helpful to look at who controls the forum in which the attack takes place [1]. There are three main sorts of forums: those controlled by the defenders, those controlled by the attackers and those controlled by third parties. The AVN controls its own Web site, SAVN controls its Facebook page, and Wikipedia, Google and the Web of Trust independently host forums in which the struggle can take place. Each forum is associated with characteristic forms of attack. These are given in Table 1, along with some defences against each method of offence.

Table 1: Three types of online methods for attacking an organisation, with typical forums, examples, possible defences and key issues raised by the mode of struggle.

Offensive method	Typical forum	Examples	Defences	Key issues
Disrupt discussions	Controlled by defender	Comments on target's blog	1. Exclude disrupters 2. Comment anonymously	Openness of discussions; number of hostile commenters
Dominate	Controlled by	Wikipedia entries; Side	1. Ignore	Accuracy of descriptions;

descriptions	independent group	Wikis; Web of Trust rating	2. Counter	responsibility for corrections
Ridicule and intimidate opponents	Controlled by attacker	Ridicule of screenshots; Hall of Shame	1. Ignore 2. Hide identities 3. Complain to authorities 4. Challenge 5. Expose	Targeting of individuals; fair play; free speech; defamation

Note that the distinction between forums is only approximate. SAVN and the AVN control their websites but these sites are potentially subject to external regulation. The independently controlled forums are subject to their own specific sets of norms, for example the rules set up by Wikipedia and the Web of Trust, which potentially could be modified due to complaints or interventions from SAVN, the AVN or others, though this is unlikely.

Several points can be made about the methods of online offence. The first is that each of these methods, in mild forms, is both common and legitimate. On nearly every controversial issue, partisans on each side try to present their viewpoints in all available forums, including forums dominated by opponents. The most common method of defence is exclusion. For example, critics of vaccination might like to post comments on the Web sites of pharmaceutical companies or government health departments, but such sites seldom have blogs and, when they do, these blogs seldom give unlimited access to critics. Critical comments are not a threat when they are a small minority of comments: the majority can counter the criticisms, thus affirming the in–house viewpoint. Disruption becomes a serious issue when the discussions are open and the disrupters have significant numbers, energy and resources compared to in–house contributors, especially when their intention is to disrupt.

Second, in this sort of struggle, formal regulations provide little or no help to the target. Most of the methods of attack are legal and within the contractual rules of Web hosts. As noted above, the methods are, for the most part, common and legitimate in mild forms, which makes it more difficult to make a case that regulations have been abused. For example, the transition from vigorous debate to unacceptable abuse is not clear–cut. Furthermore, companies such as Facebook and the Web of Trust are not well placed to intervene in disputes between competing citizens' organisations. As commercial operations, they have little incentive to invest significant energy into adjudicating the rights and wrongs of claims brought before them or for policing decisions made.

A crucial factor in the attack on the AVN is that criticism of vaccination is a non–orthodox position, with little credibility in medical and government circles. Because the mainstream medical position is hostile to the AVN, there is little prospect of receiving support from establishment bodies. If the positions of the attackers and targets were reversed, with a vaccine–critical citizens' group mounting an attack against a pro–vaccination citizens' group, it is much more likely that medical professionals and government officials would intervene against the attackers.

As a result of these factors — the attackers formally operating within the law in a situation with weak or non–existent regulation and in which official bodies are unsympathetic to the target — the target organisation needs to use its own resources. When discussions are disrupted, it is straightforward to exclude disrupters; this is the easiest type of attack to resist. When descriptions are dominated, such as Wikipedia entries, one option is to mobilise one's own supporters to promote counter–descriptions. However, when the attackers have a greater capacity for this sort of struggle, an easier option is to leave the battlefield — Wikipedia or Side Wikis — and instead focus on the quality of one's own self–descriptions, in this case the AVN's own Web presence. This can be supplemented by a description of what the opponents are doing, for example an account, on the AVN's Web site, of how SAVN and other opponents are dominating the AVN's Wikipedia entry.

Responding to ridicule and intimidation is more challenging. People join and participate in volunteer groups because they are interested in or care about the issues being dealt with. People join the AVN mainly because they want to know more about a perspective different from the orthodoxy, and to share ideas and experiences with like–minded others. Few sign up expecting to be the target of ridicule for making a blog comment. Few office bearers in citizens' organisations anticipate that their contact details will be posted online in a hostile forum. Understandably, the prospect of coming under attack deters participation.

One way to counter attacks is to expose them to wider audiences in the expectation that some people will be disturbed by the behaviour of the attackers (Martin, 2007). Some members of the public may support vaccination but be opposed to SAVN tactics. By exposing the attacks, the AVN may be able to gain greater support, not for its viewpoints but for its right to present them. It is also possible that some people, on learning about the attacks on the AVN, may want to know more about the AVN's arguments: censorship can create an interest in the thing censored (Jansen and Martin, 2003). If SAVN's efforts at destroying the AVN actually create greater attention to and wider support for the AVN, then SAVN's efforts at censorship will have backfired.

The strategy of exposing the attacks and thereby building wider support has a risk: it shifts the conceptual arena of the struggle, namely from vaccination to free speech. The AVN, by

devoting significant effort to resisting the attacks, including by using exposure of the attacks as a way of building support, may be diverted from its central mission of raising awareness about shortcomings of vaccination. On the other hand, SAVN, by concentrating on attacking the AVN, may divert the effort of many participants from a positive direction — presenting the benefits of vaccination — to the less productive enterprise of trying to squash critics of vaccination.

Conclusion

The online environment provides new incentives and opportunities for attacking citizens' organisations, including the increased importance of an online presence to organisations, the ease of coordinating attacks, and new avenues for attack created in the online environment. The result is the phenomenon of a coordinated citizens' online attack on a citizens' organisation. Online attacks are not new, being well developed by militaries and by cyberactivists. What is new here is the variety of attack methods used in a collective citizens' attempted takedown of a citizens' group.

The methods of attack described here, for example dominating a Wikipedia entry and sending adverse ratings to the Web of Trust, are specific to the SAVN–versus–AVN case study. Different methods might have been used, for example denial–of–service attacks, and no doubt in the future new sorts of methods will be developed as new social media and online tools become widely used [2]. Generalising from the case study, it is useful to classify the methods of attack into three types: disrupting discussions, dominating descriptions, and ridiculing and intimidating individuals.

The obvious response to disruption is exclusion of disrupters, a process that is conventional in moderated forums. Disruption has been a problem in online forums from the earliest days of e–mail lists; standard software for hosting blogs builds in processes for exclusion and editing, in an implicit recognition of the predictability of this sort of problem.

Responding to domination of descriptions is more difficult. When this occurs in the off–line mass media, it is difficult to counter if editors are not receptive, for example when mass media overwhelmingly describe certain groups as terrorists. In principle, Web 2.0 offers a solution: mobilise one's supporters to provide counter–descriptions. This is a reasonable prescription when the balance of forces is roughly equal, but in the face of a much larger, more energetic or better resourced opponent, the target has little chance of making editable online descriptions more balanced. This leaves two main options: ignore the dominated descriptions and concentrate on the ones directly controlled; and, expose the process of domination. The AVN has, for the most part, not tried to compete with SAVN over the Wikipedia entry on the AVN, but instead concentrated its efforts in developing and protecting its own Web site. It has not tried to document the bias in the Wikipedia entry on the AVN.

Ridiculing and intimidating individuals is often the most damaging method used. Many members of a target group are unsettled and distressed by ongoing personal ridicule; threats, explicit or implied, are even worse. The most likely result of these techniques is that many members will decline to participate openly in online forums. It is less clear whether attacks on individuals have any impact on their viewpoints. There are several possible responses to personal attacks: ignore them, make formal complaints about them, challenge them, expose them and avoid them by hiding one's identity. Hardened campaigners, who have experienced many attacks, may be able to ignore online abuse, but most citizen–group members would find this very difficult. Making complaints to agencies formally responsible for online behaviour, such as Facebook, seems to be a plausible response, but in practice it seldom provides a long–term solution. The most promising response is to document and expose the abuse to wider audiences, thereby gaining support from those who see such attacks as inappropriate.

There has been relatively little study of collective online assaults against citizen groups. There is as yet no body of evidence and case material from which target groups can learn the most effective ways of responding to attacks, perhaps because most attention has been on legal and other regulatory responses (Levmore and Nussbaum, 2010). Any practically oriented research in this area will be eagerly studied by groups that come under attack. FM

About the author

Brian Martin is Professor of Social Sciences at the University of Wollongong, Australia.
Web: http://www.bmartin.cc/
E–mail: bmartin [at] uow [dot] edu [dot] au

Acknowledgements

For discussions and valuable comments in response to drafts, I thank Kevin Dew, Meryl Dorey, Ted Mitew, Sian Morton, Florencia Peña, Kirsti Rawstron and Danny Yee. For helpful textual suggestions, I thank Trent Brown, Frank Huang, Julia Najjar and Majken Sørensen. None of these individuals necessarily agrees with the views expressed here.

Notes

1. I thank Danny Yee for suggesting this perspective.

2. Twitter is another medium that has been used in the vaccination debate, but is not addressed here.

References

F.E. Andre, R. Booy, H.L. Bock, J. Clemens, S.K. Datta, T.J. John, B.W. Lee, S. Lolekha, H. Peltola, T.A. Ruff, M. Santosham, and H.J. Schmitt, 2008. "Vaccination greatly reduces disease, disability, death and inequity worldwide," *Bulletin of the World Health Organization*, volume 86, number 2, pp. 140–146, and at http://www.who.int/bulletin/volumes/86/2/07-040089/en/, accessed 1 December 2012.

Jeffrey Carr, 2012. *Inside cyber warfare*. Second edition. Sebastopol, Calif.: O'Reilly.

Karl von Clausewitz, 1832–1834. *Vom kriege*. Berlin: Ferdinand Dümmler.

Digital Activism Reseach Project, "Civil resistance 2.0," at http://digital-activism.org/index.php/for-activists/cr20/, accessed 3 December 2012.

Barney G. Glaser and Anselm L. Strauss, 1967. *The discovery of grounded theory: Strategies for qualitative research*. Chicago: Aldine.

Louise Kuo Habakus and Mary Holland (editors), 2011. *Vaccine epidemic: How corporate greed, biased science, and coercive government threaten our human rights, our health, and our children*. New York: Skyhorse.

Richard Halvorsen, 2007. *The truth about vaccines: How we are used as guinea pigs without knowing it*. London: Gibson Square.

Pru Hobson–West, 2007. "'Trusting blindly can be the biggest risk of all': Organised resistance to childhood vaccination in the UK," *Sociology of Health & Illness*, volume 29, number 2, pp. 198–215.

Lech J. Janczewski and Andrew M. Colarik (editors), 2008. *Cyber warfare and cyber terrorism*. Hershey, Pa.: Information Science Reference.

Sue Curry Jansen and Brian Martin, 2003. "Making censorship backfire," *Counterpoise*, volume 7, number 3, pp. 5–15.

Tim Jordan, 2002. *Activism! Direct action, hactivism and the future of society*. London: Reaktion Books.

Herman Kahn, 1961. *On thermonuclear war*. Second edition. Princeton, N.J.: Princeton University Press.

Saul Levmore and Martha C. Nussbaum (editors), 2010. *The offensive Internet: Privacy, speech, and reputation*. Cambridge, Mass.: Harvard University Press.

Brian Martin, 2007. *Justice ignited: The dynamics of backfire*. Lanham, Md.: Rowman & Littlefield.

Martha McCaughey and Michael D. Ayers (editors), 2003. *Cyberactivism: Online activism in theory and practice*. New York: Routledge.

Hellen Megens and Brian Martin, 2003. "Cybermethods: An assessment," *First Monday*, volume 8, number 2, at http://firstmonday.org/article/view/1035/956, accessed 1 December 2012.

Paul A. Offit and Louis M. Bell, 2003. *Vaccines: What you should know*. Third edition. New York: Wiley.

Justin W. Patchin and Sameer Hinduja (editors), 2012. *Cyberbullying prevention and response: Expert perspectives*. New York: Routledge.

Marcella Piper–Terry, 2011. "Happy birthday, Max. Here's your sign" (4 August), at http://vaxtruth.org/2011/08/happy-birthday-max-heres-your-sign/, accessed 9 August 2011.

Greg Rattray, 2001. *Strategic warfare in cyberspace*. Cambridge, Mass.: MIT Press.

Reporters Without Borders, 2005. *Handbook for bloggers and cyber–dissidents*. Paris: Reporters Without Borders, at http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf, accessed 1 December 2012.

Gene Sharp, 1973. *The politics of nonviolent action*. Boston, Mass.: Porter Sargent.

Mao Tse–Tung, 1961–1965. *Selected works of Mao Tse–Tung*, volumes 1–4. Beijing: Foreign Languages Press.

Wim van de Donk, Brian D. Loader, Paul G. Nixon, and Dieter Rucht (editors), 2004. *Cyberprotest: New media, citizens, and social movements*. London: Routledge.

Editorial history

Received 7 April 2012; accepted 30 November 2012.

Online onslaught: Internet–based methods for attacking and defending citizens' organisations by Brian Martin
First Monday, Volume 17, Number 12 - 3 December 2012
http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/4032/3379