Feminist Cyber-resistance to Digital Violence: Surviving Gamergate

Macarena Hanash Martínez

ABSTRACT

Women in cyberspace do not escape patriarchal violence and are subject to strict social control exercised through technological means. Cyber-violence especially affects women with an explicitly feminist presence in virtual spaces. Their participation in and advocacy of feminist values are considered a transgression of the patriarchal mandate, which seeks to exclude women from public spaces or, failing that, to marginalise them. That is why they are the targets of grave intimidation, harassment and threats. At the same time, digital networks have spawned a plethora of spaces for women’s collective, political and social action. Thus, online activity has played a key role in the resurgence and revitalisation of feminist communities and debates. This paper analyses the projects launched by Zoë Quinn and Anita Sarkeesian, two of the main targets of the Gamergate movement. We will study: (1) Crash Override and Speak Up & Stay Safe(r), a helpline and a resource platform for cyber-violence victims, respectively; (2) feminist cyber-resistance projects, within the framework of cyber-feminism and the current paradigm shift in the culture of protest and feminist organisation.

Keywords: cyber-feminism, cyber-violence, manosphere, Gamergate.

INTRODUCTION

August 2019 marked the fifth anniversary of the beginning of Gamergate, a massive campaign harassing feminists under the pretext of defending journalistic ethics in the tech and video-game industries. The Gamergate movement sprang to life in 2014, sparking a fierce cultural war that has raged until the present. On the one hand, there were video game critics and independent (‘Indy’) creators — most of them women — who demanded greater inclusion in the industry. On the other hand, there was a mixed bag of opponents: journalists, anti-feminist groups, YouTubers, influencers, trolls, and even conspiracy theorists. Yet in reality, Gamergate was a side-show
to the main cultural battle for an Internet space that would both make women visible and include them.

The Gamergate events were not the first sign of Internet-spawned violence against women. Similar attacks had been carried out before this major harassment campaign — as we shall see later, and had a particularly racial twist. In 2013, for example, in what came to be known as ‘Donglegate’, the consultant Adria Richards tweeted a sexist joke that she had heard at a technology conference she had attended. The tweet ‘went viral’, she was sacked and private/identifying information on her was bandied around the Internet. As a result, Richards received death threats, while ‘touched up’ photos of her were published in which her head was grafted on to the torso of a naked porn queen. Indeed, some months before Gamergate, 4chan users got together, pretending to be online feminist women, sparking a new trend of fake feminist hashtags such as #EndFathersDay and #WhitesCan'tBeRaped (Warzel, 2019). These hashtags can be thought of as part of a larger ‘misinformation campaign’ but they are not the only case in today’s highly-charged political and social scene. Strategies based on the kind of misrepresentation and violence seen during Gamergate also played a part in smoothing Donald Trump’s path to The White House. This was because the online mobilisation of the ‘Alt-Right’ [Alternative Right] did much to sway swing voters. Indeed, the key figures in this new American Right such as Milo Yiannopoulos, Mike Cernovich, and Steve Bannon became celebrities and consolidated their fan base at the height of Gamergate. The discussions of conspiracy theories by Trump followers seen in other Internet scandals such as Pizzagate and QAnon are hosted on the same web pages as back then. Today, these web sites continue to churn out anti-feminist attacks. For instance, 8chan, a web site that played a big role in Gamergate was closed after it featured in no fewer than three mass shootings in 2019 — El Paso (Texas, US), the Christchurch mosque (New Zealand) and the Poway synagogue (California, US). The shootings were all announced previously on the web site’s forum by the respective killers. The radicalisation of White ‘straight’ [heterosexual] men to right-wing/ ‘Alt-Right’ positions on web platforms such as YouTube and Reddit (Horta Ribeiro et al., 2019; Habib et al., 2019) is something that feminists (as victims of digital violence) have denounced for years. Here, feminists argue that such virtual violence is often a harbinger of the real thing, fostering hatred of women, racial minorities, members of certain faiths, and the LGBTQ community in general. Feminists further argue that such violent discourse is commonly found on ‘men only’ sites (which they dub the manosphere). These sites form a realm of blogs, forums, web sites, sub-Reddits, and Twitter, YouTube, and Facebook accounts. The realm’s common denominator is hatred or resentment of women in general and of feminists in particular. The manosphere shifted from cyber-culture’s fringes to the centre between 2010 and 2014, beginning with the social network culture and ending in the Gamergate saga (Jane, 2018). Unwilling male virgins, ‘men’s rights’ activists, pick-up artists, and Crypto-Nazis (those who express their Nazi beliefs in ‘code’ yet deny that they are Nazis) all share a sub-culture, a set of aims, the same anti-feminist, racist language and ideology, and Neo-Darwinist, Neo-Liberal principles.

Given its scale, media impact, and ramifications, Gamergate is considered a paradigmatic case. That is because the cyber-attacks were made against: (1) women around the world (especially those in the video game and IT industries); (2) feminist writers and journalists covering/denouncing Gamergate (such as Jenn Frank, Mattie Brice, Brianna Wu, Jessica Valenti, Ijeoma Oluo, Ellen Pao, among many others). In particular, we study the cases of Quinn and Sarkeesian and the cyber-resistance strategies feminists came up with to survive Gamergate. To this end, we used a qualitative methodology based on ‘netnography’ [net-based ethnography] (González Gil and Servín Arroyo, 2017) since the Internet is not only a space in which culture is (re)produced but is also a cultural product stemming from social practice.

This method centres on the study of online spaces, which is to say on human relations, digital com-
Communities and culture. Thus ‘netnography’ gave us practical ideas for gathering, producing, and analyzing data on both the ‘manosphere’ and feminist cyber-resistance. In both cases, we apply one of the four ways of using netnography indicated by Kozinets (2015), In symbolic netnography, one makes a craftsman-like search of key webs and profiles to grasp meaning systems in the online field. As Christine Hine notes, “Internet ethnography [netnography] does not necessarily mean moving from one’s desk”. The netnographer visits web sites to gain insights into the nature of users’ experience, not to travel” (2004: 60). Putting traditional ethnographic tools to work in the digital world involves beginning with a little cultural familiarisation to facilitate the subsequent fieldwork. Browsing and reading the content in the ‘manosphere’ and cyber-feminists responses to it helped us compile a list of the most important webs for the purposes of our study. During this period, we drew up a list of cases on digital violence against feminists, from which the two cases covered by this paper were chosen. We examined the responses provoked by this violence and their outcomes. As Pink et al. (2016) note, the digital aspect is not the most important feature of ‘netnography’. That is because online relations are not confined to the digital sphere since they also reflect and spill over to offline settings and their socio-cultural conditioning factors and socio-cultural patterns. This means that what interests us is the interaction between people and technology and the interrelationship between online and offline spheres. Because these interactions are complex, they cannot be seen as mere dichotomies. Accordingly, the paper considers the unfolding of events both within and outside the digital sphere to reveal how cyber-violence is an issue that reaches beyond the computer screen.

CIBER-VIOLENCE: A PHENOMENON PENDING DEFINITION
Feminist literature reveals sundry notions on what constitutes cyber-violence in the digital sphere and uses a plethora of terms to describe it. These terms include: ‘cyber-violence’; ‘cyber-abuse’; ‘online abuse against women and girls’; ‘technology-aided gender violence’; ‘online hate’; ‘e-bile’; ‘gender trolling’; ‘online misogyny’, and (more exotically) ‘rapeglish’ (Banet-Weiser and Miltner, 2016; Citron, 2014; Ging, 2017; Ging and Siapera, 2018; Jane, 2014, 2018). Some of these are broad umbrella terms, others are gender-neutral. In general, the terms are limited in one or more ways depending on the cases they are applied to, the nature of the victims, the aggressors, and the kind of violence employed. On the one hand, this lack of consensus reveals the novel, complex nature of the phenomenon. On the other hand, it gives a wide range of options for analysing the issue. Here, one should note that online male chauvinist violence may also have racist, homophobe, or transphobic dimensions if the women attacked are ‘racialised’, belong to the LGBTQ group, or to other marginalised minorities.

In 2007, Amnesty International conducted a study into online violence against women. It covered eight countries. No less than 23% of the women surveyed stated that they had been subject to some kind of online abuse or harassment, while almost half (46%) said that the violence was of a sexist or misogynist nature. When it comes to the perpetrators, 60% of women were the victims of unknown aggressors. The kind of violence seen in Gamergate has a set of common features, namely it: (1) takes place on the Internet; (2) makes use of anti-feminist propaganda; (3) is long-lasting; (4) it is collective and anonymous, making it possible to ‘specialise’. Digital violence makes use of sundry strategies to reach its goals. These strategies include: (a) sexist insults; (b) hate speech; (c) ‘flaming’ (starting discussions with offensive messages — usually in forums); (d) unsolicited messages of a sexual nature; (e) stalking and monitoring; (f) harassment; (g) threats; (h) identity theft; (i) libel; (j) vengeance porn; (k) sexual blackmail; (l) ‘doxing’; (m) ‘swatting’ (making hoax calls to emergency services; (n) hacking; (o) Denial of Service (Dos) / Distributed Denial of Service (DDoS) attacks; (p) ‘pharming’ —that is, redirecting a domain name to another page; (q) ‘outing’ (revealing another person’s sexual identity); (r) ‘deadnaming’ (using the birth name of a trans-
sexual individual); (s) ‘Google-bombing’ (changing the search index results in Google); (t) ‘shock trolling’ (using frightening contact to shock victims), and so forth. In addition, one should note that some of those who have suffered digital violence made use of one or more of the precautionary measures set out in this paper. Attackers often use several strategies at the same time. It is therefore impossible to say where one ends and another begins — something that makes the subject that much harder to study.

Thus ‘raiding’ (a massive, co-ordinated attack) was common during Gamergate and was typical of anonymous forums such as 4chan. These attacks comprised insults, threats, touched-up photos sent by e-mail, and messages sent by text or through social networks. The purpose of such violence is to silence, marginalise, or expel women from the public sphere (whether this be online or offline). In the case studied in this paper, the targets of the violence were women who were explicitly feminist in a sphere dominated by men — that of video games and technology. According to the 2017 Amnesty International Report, cyber-violence has a ‘chilling effect’, discouraging women from exercising their rights because they are fearful of legal sanctions, being constantly stalked, are racked by anxiety, self-censor, distrust others, feel panic, suffer from post-traumatic stress, seek high-level security, and so on. One of the Report’s findings was that women feared for their safety in the real world in 41% of cases. With regard to the effects of violence, 58% of women victims said they were afraid to use the Internet and/or social media again. Furthermore, 56% of the women surveyed said that they were less able to concentrate on daily tasks, and 55% suffered stress, anxiety, and panic attacks. Furthermore, two thirds of the women felt helpless in the face of such violence. Most women (76%) changed the way they used social networks as a result so as to boost their security and privacy, changed the content of what they published, or the expressions they used — in other words, online violence elicited a kind of self-censorship. This is where cyber-feminist resistance strategies come into play to battle against and survive digital violence.

**Cyber-feminism: dwelling online**

The patriarchy — says Sadie Plant (1996) — is not a construction, order, or structure but rather an economy in which women are staple goods. It is a system in which exchanges take place solely among men. Women, tokens, merchandise and money always pass from one man to another and it is assumed that women exist “solely as a medium, transaction, or transfer between a man and his fellows” (Irigaray 1985b: 193; cited in Plant, 1996: 341). This ‘speculative economy’ is underpinned by tools, basic products, and the media knowing their places and having no aspiration to usurp or subvert the governing role of those they serve. The patriarchy needs to contain and control what is meant by ‘woman’ and ‘feminine’.

Nevertheless, the digital sphere took off in the mid-1990s and the Internet grew, becoming a melting pot of old identities. Gender could be bent and blurred and space-time co-ordinates meant little. Virtual worlds are not only important because they open up existing spaces to women within a given order of things but also because they undermine a vision of the world shaped by “two thousand years of patriarchal culture” (Plant, 1996: 340). Plant stresses the creative potential of cyber-space, a place where one can transgress and challenge the patriarchal economy and threaten to dissolve subjectivity (Kennedy, 2007).

For Plant, “technology is basically feminine” (A. Guil Bozal and J. Guil Bozal, 2006: 84). She goes further and argues that co-operation between women, machines, and technology is the basis of cyber-feminism. In her words: “Cyber-feminism is an uprising by goods and materials in the patriarchal world; a dispersed, networked rebellion forged through links between women and computers, and between computers, communication systems, and networks” (1996: 349).

One cannot speak of cyber-feminism without mentioning Donna Haraway. In her work *Ciencia, cyborgs y mujeres: la reinvención de la naturaleza*, the author looks at the position occupied by women’s bodies in what she terms “the computing science of domination”, a world production, reproduction, and communica-
Feminist theory in general and cyber-feminism in particular owe their concept of cyborg to Haraway. She states that “ICT and biotechnology are key tools for building our bodies” (1995: 279). Haraway uses the imaginary of the cyborg as a metaphor, symbol, and representation to escape from facile dualisms of gender, race, and class. A cyborg is defined as “a cybernetic organism, a hybrid whether machine and living thing, a creature spawned by social reality and by fiction” (1995: 253). A central utopian discourse on technology and computers gives people the chance to escape their bodies (Lupton, 1995). The notion of a cyborg is the closest there is to this ideal, and thus represents the idealised body.

According to Plant (1998), bodies are continually shaped by the processes they are subjected to. Yet in the Internet, these processes have no material limitations. In Plant’s scheme, the Internet is a space without bodies that holds out the promise of a sphere in which one has total freedom, a place “that is limitless in terms of the names one can use. An individual can spawn a host of avatars on the Internet, and these may assume any sexual identity or species” (1998: 52). The possibility of discarding our bodies in this sphere is just one more step towards building a post-gender world and achieving the cyborg ideal.

This is seen as a utopian position within the cyber-feminist movement given that it does not matter how virtual the subject is, there is always a body
linked to it wherever it may happen to be (Stone, 1992). This is especially true of the feminists whom we analyse here, no matter how much they carry out their professional activities in cyber-space; their physical, gendered bodies are always present. Even though they come up with new ways to shed their ‘offline’ bodies, one should note that the virtual community springs from the physical world and must return to it: “Even in the era of the techno-social subject, life is lived through bodies” (Stone, 1992: 452). Forgetting the body is physically harmful (especially for women from racialised minorities and others pushed to society’s fringes).

Zafra (2004) also argues that cyber-space should be seen as a new way of forging communities. It is an interactive, multi-dimensional medium in which users can be spectators, producers, and spreaders of information all at the same time. Furthermore, cyber-space’s cross-cutting, de-hierarchicalised nature lends itself to a liberating, creating use of the medium. This allows one to ‘de-territorialise’ and ‘re-territorialise’ experience and lay claim to one’s localism or globalism, as the case may be.

In addition, “Internet as a political sphere makes many think in terms of a utopian collectivism uniting Mankind within a single overarching network” (Zafra, 2004: 65). Yet the Internet also threatens to repeat or strengthen the patriarchy’s socio-symbolic patterns. For women (a group historically kept out of the public sphere) the use of the Internet for feminist political purposes poses many opportunities and challenges. Cyber-feminists are the first to acknowledge that “ICT has great potential for making a personal, educational, and political impact, opening up new possibilities for women to challenge traditionally-defined roles for the fairer sex and to break down the hang-over of organisational rules rooted in the past” (2004: 74-75). Like in the feminist self-awareness groups of the 1970s, today’s Internet also exhibits a confluence of public and private spheres. From the cyber-feminism standpoint, re-thinking women’s role online involves coming up with new ways of shaping the subject, and new ways of building the collective. On the one hand, subjects with or without projected or invented bodies can ditch the built identities that bind us. On the other hand, online settings for the collective — what Zafra calls “action micro-spaces” (2004: 99) — let us leap spatial boundaries and thus also overcome the confluence of different cultures and contexts. In any event, this social cyber-structuring of collectives and subjectivities requires feminisation — in the form of de-hierarchicalisation and deconstruction (2004: 95) of the patriarchal, hegemonic mindsets of ‘the powers that be’.

**GAMERGATE: THE CASES OF ANITA SARKEESIAN AND ZOE QUINN**

In February 2013, Zoë Quinn, a designer of independent video games, launched *Depression Quest*, an interactive game that related a young person’s history of depression. The game enjoyed little success at the outset but it did spark debate on Wizardchan (an Internet forum for virgin adult men). Forum members complained about the poor quality of the game and that women could not be expected to grasp the nature of ‘real’ depression. Some of the forum users found Quinn’s telephone number and began calling her. She documented the insults hurled at her on social networks (but not against the game’s co-author, who happened to be a man) (Malone, 2017). In August 2014, her former boyfriend, Eron Gjoni, created a blog titled thezoepost.wordpress.com, in which he described intimate details of his relationship with Quinn and accused her of having screwed positive reviews out of journalists in the video-gaming sector in return for sex (Totilo, 2014). One of these men was Nathan Grayson, a writer for Kotaku, a leading web site in the field. Yet the fact is that neither Grayson nor Kotaku published reviews of Quinn video game. That, however, did not stop thousands of users flooding the social networks (see Figure 1) with messages such as: “If I ever see you at an event Round Table, I will kill you. You are not worth shit and you deserve to be hurt, to be mutilated, and killed. I will piss on your rotten corpse a thousand times over” (Malone, 2017).
What was to become a massive cyber-harassment campaign against Quinn was set in motion on /pol/ Politically Incorrect, a discussion board on the anonymous 4chan forum. The title given to the threads was ‘Ethics in Game Journalism’ to ward off possible criticism. The idea was to seize on lack of journalistic ethics to forge a supposedly reformist movement and to criticise the elimination of the sub-forum as stemming from censorship or poor moderation. Quinn’s former boyfriend was invited to the sub-forum and this is why ‘Quinnspiracy’ was the name given to what was later to be known as Gamergate. Gjoni’s involvement made it clear that the protests had little to do with journalists supposedly breaking their code of practice. Shortly after Gjoni’s accusations, some hackers revealed personal documents on Quinn and photos of her stark naked. Her Wikipedia entry was altered and her open death date was first change to ‘soon’ and then to the date of her next public appearance. Furthermore, Quinn’s father’s address was leaked. He received so-called ‘cum tributes’ in due course with photos of his daughter covered in semen (Malone, 2017). Quinn obtained a restraining order. Yet given the gravity and credibility of the rape and death threats, she was forced to leave home (Dewey, 2014). As a result of these attacks, Quinn was diagnosed with complex post-traumatic stress, a problem that compounded her previous mental problems — something that Gjoni used against her. In Autumn 2016, Quinn dropped the charges of harassment even though the Courts had banned posts on her. That said, the legal system was virtually powerless to stop the growing horde of cyber-freaks harassing her. During the hearings, a judge who saw no legal grounds for harassment went so far as to suggest Quinn look for a job that caused her less grief. His advice was: “You are a smart girl [...] do something else” (Malone, 2017).

The case of Anita Sarkeesian — a Canadian culture critic — may be better known than that of Quinn in the Gamergate saga. In 2009, a website titled Feminist Frequency was created together with a set of videos in order to analyse and criticise stereotypical portrayals of women in popular culture, and in games and in online spaces. Three years later in 2012, it was decided to launch a crowd-funding campaign on Kick-starter to fund Tropes vs. Women, a series of YouTube videos in order to research the tropes applied to female characters in popular culture, such as ‘the damsel in distress’, the ‘manic pixie dream girl’, and ‘Woman in the Refrigerator’. The project raised over US $150,000 — much more than the US $8,000 target set (Campbell, 2017). The reaction in the ‘manosphere’ to this runaway success was to accuse Sarkeessian of fraud and pocketing some of the money raised. From 4chan and subreddit The Red Pill, ‘raiding’ campaigns were set in motion against the crowd-funded campaign. These ‘raids’ included flooding the social networks with death and
rape threats (Figure 2) and altered images showing the targeted women being sexually abused. For instance, Benjamin Daniel, a self-styled ‘feminist-basher’ created Beat Up Anita Sarkeesian, a video game that lets users bash a picture of Sarkeesian’s face (Ging, 2017).

In September 2014, the organisers of the Game Developers Choice Awards received bomb threats if they gave Sarkeesian an award as industry ‘ambassador’. On this occasion, special security measures were taken for the event. Nevertheless, a conference at Utah University the following month had to be called off because of threats. An e-mail signed by someone who claimed to be a student threatened to carry out America’s most deadly campus shooting [sadly, not an easy record to beat]. “One way or another, I will make sure they all die”, wrote the author, threatening to gun down conference-goers, staff, and members of the university’s Women’s Centre (McDonald, 2014).

More recently, at the VidCon convention in June 2017 (the world’s biggest event of its kind in the field), brought together thousands of people working in the online video industry. Sarkeesian took part in the Women Online Round Table (Kane, 2017). Carl Benjamin — the British YouTuber hiding behind the online pseudonym ‘Sargon of Akkad’ was sitting near the front with a group of his followers. Benjamin can be thought of one of the most ‘professional’ harassment artists of those mentioned earlier. That is because he makes over $5,000 a month through his Patreon site, with a network of subscribers or ‘patrons’ eagerly lapping up his incendiary videos attacking a number of victims, including Sarkeesian. There are many YouTubers who make a handsome living out of ugly videos that vilify and mock feminists such as her. A number of unscrupulous souls eager to make a quick buck are taking advantage of a new market niche, to wit the online harassment industry with an anti-feminist twist. Taken as a whole, these accounts have millions of followers whose threats and harassment are spurred on by a constant stream of videos spreading lies and inciting violence.

Figure 2 Examples of the tweets received by Sarkeesian

At the time of writing, Benjamin has 963,000 subscribers to his YouTube channel. His content covers various political subjects in The United States and The United Kingdom: Black Lives Matter; racism; terrorism; freedom of speech and so on. Most of his videos rail against the ills of feminism, the Liberal elites, the media, ‘political correctness’ (sic), and in general all the ‘left-wing reactionaries’ he considers responsible for repressing free speech (Campbell, 2017). Furthermore, in line with other anti-Feminist propaganda, he stoops to using ‘Photoshopped’ pictures of Sarkeesian in his videos (Figure 3). Before he was expelled from Twitter, his ‘Wall’ page used an unflattering mash-up of a picture from Disney’s Beauty and The Beast to snipe at his victims (Figure 4).

During the VidCon events, Benjamin gate-crashed a Round Table featuring various women, including Sarkeesian, Kat Blaque, and Franchesca Ramsey (the latter two being both activists and YouTubers). Benjamin was accompanied by a cameraman and a posse of followers who then interrupted the proceedings and made things difficult for the speakers. The gatecrashers’ actions were acts of deliberate harassment and intimidation.

The Round Table began with the question: “Why do we need to discuss online feminism in video games?” to which Sarkeesian answered: “Because those harassing me are sitting in the front row”. After the event,
Benjamin went on to the social networks and uploaded a video alleging that he had been insulted. He said that Sarkeesian had called him “human refuse” and “a wanker”, and that this ran counter to VidCon’s guidelines. He lamented that Sarkeesian had refused to hold a debate with him. Following the video posting, there was a spate of violent insults against all those who had taken part in the Round Table. Sarkeesian wrote on her web site: “It was a deliberate attempt to poison the atmosphere and show us that if we dare to appear in public to express the ideas that we share online, then we can expect the harassment we suffer on social media to pursue us into the physical world” (Sarkeesian, 2017).

In his video reacting to the events at VidCon, Benjamin said that the first three rows in the audience were filled with his followers, who proudly call themselves shitlords, the sworn enemies of the SJW. He added that his actions were not ill-intentioned but merely ‘playful’: “We had a ball. It was an adrenaline rush to be there to engage in shit-posting and to troll” (cited in Campbell, 2017). In this respect, Sarkeesian said that these statements bore out what she had been saying for years: “They are doing all this just for the hell of it. They get a kick out of using the power the patriarchy has given them to ‘put women in their place’, to intimidate and silence those who dare raise their voices and uphold their right to be treated with respect and decency in these spheres and to live full lives” (cited in Campbell, 2017).

Nevertheless, she said that for her and other women, being the target of these harassment campaigns is a worrying, traumatic experience. Indeed, extra security had to be laid on during the rest of the convention. In confronting Benjamin, Sarkeesian said she wanted to dispel the idea that women should avoid conflict and remain passive when threatened. She argued that ‘turning the other cheek’ silenced women’s voices, thus perpetuating a culture in which such harassment is seen as normal. “I believe the row was liberating for those women who grasped what happened and who had been through the same thing themselves. They could see that I did not just take it on the chin but instead directly challenged the shitlords to admit what they had done” (cited in Campbell, 2017).

Feminist Cyber-resistance: Life beyond Gamergate

In 2015, Anita Sarkeesian created the web page Speak up & Stay Safe(r) in collaboration with Jaclyn Friedman and Renee Bracey Sherman. The web site provided an online guide for protecting oneself against online harassment. Friedman calls herself “a feminist agitator” and is an activist and the author of several books: Yes Means Yes: Visions of Female Sexual Power and a World Without Rape (2008) and What You Really Want: The Smart Girl’s Shame-Free Guide to Sex and Safety (2011). She is also the founder and former Director of Women, Action & the Media (WAM!), a non-profit organisation focusing on the struggle for gender justice in the media. Renee Bracey Sherman is an activist for reproductive justice. She sits on the Board of the pro-rights reproductive organisation NARAL Pro-Choice America. Sherman is also the author of the work Saying Abortion Aloud: Research and Recommendations for Public Abortion Storytellers and Organisations.

Speak Up & Stay Safe(r) was created with the stated goal of sharing what these three women had learnt after years of being victims of digital violence: “We know how intimidating, terrifying, and overwhelming online harassment can be and we hope that this document helps empower women readers take informed decisions on security and preventative measures” (Friedman et al., 2017). The web site is in three languages: English, Spanish, and Arabic. The Project is one that is constantly evolving. At the time of writing, the last update to the web site was July 2018. Yet the document is also one that is open to collaboration by others, especially when it comes to translation into other languages. The documents and resources on the web site were gathered with the help of experts in online security and other fields. According to Sarkeesian, this guide is for anyone who has suffered a cyber-attack or who fears they will. It was specially designed for women,
racialised people, trans-gender individuals, ‘queer’ people, and others whose oppression is aggravated by digital violence (Sarkeesian, 2019).

One should note that Sarkeesian, Friedman and Bracey Sherman stress that their guide is neither infallible nor free from bias, warning readers that:

We wish that there was no need to write this guide. You should take at least some of these precautions to ensure your safety online. Unfortunately, this will cost you time and maybe even some money but this is the price that women, and coloured, queer, and trans-gender folk and members of other oppressed groups have to pay to dare to express their opinions in public [...]. We also note that people with greater economic privileges and leisure time find it much easier to exhaustively apply such strategies. This fact of life is itself a structural injustice, underlining the unfairness of online harassment. No system is foolproof so there is always a chance that one may still fall prey to harassment despite taking all the recommended precautions (Friedman et al., 2018).

The guide is easy to follow and users do not need any special skills to apply the recommended steps. Any user with a basic knowledge of computers and the Internet will be able to put its recommendations into practice. At the outset, the document states that it gives guidance on how one can protect oneself from individuals, poorly-organised groups, and cyber-mobs online. If the attackers are governments, large companies, or well-organised institutions, users are recommended to use Front Line Defenders — an organisation that focuses on defending and protecting Human Rights activists in peril.

The guide comprises eleven main sections:

• Recommended preventative measures. These include ones to prevent doxing such as accessing data broker pages\(^5\) to check one’s personal information available online and to delete it whether by making a formal request or by creating an account that removes your information from those lists. Furthermore, doxing attacks usually also target people in the victim’s circles in order to amplify the impact of harassment. That is why it is recommended that friends and family also take measures to protect their personal data.

• Secure passwords and access. This section recommends: (1) having many different passwords; (2) changing passwords often; (3) using an online password manager; (4) creating long, difficult passwords; (5) making sure these are never saved in ‘the cloud’; (6) using two-factor verification; (7) using security questions; (8) using different e-mail addresses for different accounts.

• Security on web sites: This includes security advice to protect web domains and the comments section, as well as how to protect oneself against DDoS attacks and the risks involved in using certain plug-ins and widgets.

• Social networks: Given that many feminists use social media to complement their own networks, this section makes recommendations on such media sites, such as how to: (i) de-activate geo-localisation; (ii) check what is published on one by monitoring the alerts and notifications such as those provided by Google Alerts (iii) making reverse searches for images if one is worried about a given image; (iv) creating accounts with one’s own name on a major platform. The section also includes tips and guidance on browsing Facebook and Twitter and on using these social networks safely.

\( ^5 \) Data brokers are companies that gather information on people from public and/or private sources, add anonymous individual profiles, and then sell the data to marketing and advertising companies, government agencies, insurance companies, and outer outfits.
• Security in online gaming: Recommendations on passwords, gamer tags, profiles, accounts, privacy controls, downloads and re-broadcasting in streaming mode for gamers.

• ‘Snail Mail’ (letters, parcels): As we noted earlier, attackers can also use strategies to physically threaten users in the offline world. That is why the authors tell users how to protect themselves from attacks using snail mail and postal addresses — for instance, using mail boxes rather than street addresses, or so-called ‘virtual mail boxes’.

• Other: This section gives tips on such things as creating aliases, camera security, video calls and chats, encrypting devices such as cell phones, laptops, and tablets.

• Documentation and denunciation: The authors highlight the importance of documenting harassment and denouncing it to the social networks and platforms on which it takes place, and to the authorities.

• Strategies based on the individual: This section suggests drawing up communication plans, supporting friends, family, colleagues, and staff. There is also a sub-section on keeping oneself healthy in body and mind.

• Resources: Given that the guide does not cover all the resources available, this section introduces new tools, including those provided on the Crash Override web site, which we shall look at below. This helps fill some of the gaps should users need a wider range of options.

• The final section on online harassment provides links to books, videos, and articles covering online violence in greater depth.

In addition, based upon their experience as victims of cyber-violence, Zoë Quinn and Alex Lifschitz (the latter another video-game developer who was harassed in the Gamergate scandal), founded Crash Override in 2015. The organisation is a helpline, a non-profit, and a resource centre all rolled into one, helping those who have suffered or are suffering online violence. Crash Override comprises a network of experts and ‘survivors’ who work with victims, tech companies, legislators, the media, experts in security and mental health, and the security forces to heighten public awareness of the issue and to provide direct help with a view to eliminating the causes of online violence. For reasons of privacy and given the risk that fighting such violence entails, the people working in the organisation remain anonymous as far as the outside world is concerned. The entity tackles a range of issues, including sex photos/videos (vengeance porn); hacking; online security; harassment; stalking; doxing; swatting; identity theft; threats; cyber-mobs; hate speech groups. Crash Override offers resources to individuals, groups, companies, and Civil Servants. The organisation supports victims before, during, and after violent episodes, drawing on public resources, private help, and collaboration with other bodies to address the problem. To this end, Crash Override furnishes guides, interactive tools, and educational materials covering online violence, information on protection and security measures. These resources cover the basic features of violent events. Nevertheless, each act of violence is unique, making victims believe no one else has the same problem. This makes them feel even more alone and helpless. That is why Crash Override has free private helplines for victims. Personalised help includes a ‘safe space’ in which victims are listened to, understood, and helped by expert staff members or by those who have suffered similar violence. The victims are helped on: (1) avoiding or confronting violence; (2) dealing with stalkers; (3) denouncing abusive social network accounts; (4) post-query monitoring and support; (5) referral to specialists and/or other organisation when Crash Override lacks the resources or skills to deal with an issue. On the last point, one should note that the network is staffed by volunteers — something that inevitably imposes limitations.

They work with technology companies to forge communication channels to speed up action on users’ complaints and thus cut the time taken to deal with harassment on social media platforms. In addition,
both sides benefit from this collaboration. On the one hand, the network gets to know the internal workings of social media companies (thus helping *Crash Override* improve its support for victims). On the other hand, the social platforms use the feedback from *Crash Override* to tighten up on the terms of use and service, and ensure they are complied with. This is the case of Civil Servants, government agencies, legislators, and security forces, whose experts help draw up policies to protect those subject to online violence — especially when the culprits are former husbands and boyfriends. Furthermore, when companies, activist organisations, government and judicial bodies work together, this makes it easier for individuals to work with the network and to take part in a long-term informal study looking at ways to fight online violence.

Last but not least, the resource centre offers guides on safety, doxing, communication with the police and similar bodies, educational materials for staff, guides for third parties — which for example includes *Speak Up & Stay Safe(r)*, and a list of useful tools to round off one’s online protection. These additional tools and applications include such things as password managers, and two-factor verification. One of these tools is C.O.A.C.H (*Crash Override’s Automated Cybersecurity Helper*) (Figure 5), an interactive application that takes users step-by-step

![Figure 5](image-url)
through the process to protect every aspect of their online presence.

In addition, one should also note that Feminist Frequency became the tax sponsor of Crash Override in 2016 (Sarkeesian, 2016). Nevertheless, in its 2018 Annual Report, the organisation stated that the Crash Override team would henceforth form part of other groups even though the web site and C.O.A.C.H. guide continue to operate (Feminist Frequency, 2018).

**FINAL REFLECTIONS**

To sum up, Gamergate can be seen as a paradigmatic example of anti-feminist digital violence. Gamergate was a watershed, attracting a great deal of media and social attention — especially in The United States. Violence against women in general and against feminists in particular grew greatly during Gamergate and increasingly focused on the digital sphere. This reprehensible conduct led to much more discussion on social platforms and web sites’ responsibilities to the online community, and on the means available to the judicial to pursue such violence. Since the lamentable events of 2014, certain web sites such as Twitter, Spotify, and Paypal have drawn up new policies and have expelled leading ‘manosphere’ figures behind the harassment campaigns. Other social media providers such as Facebook, YouTube, and Reddit, continue to host and protect individuals and groups bent on spreading hate and inciting violence.

Cyber-feminism faces challenges on many fronts. One problem is that some platforms are working at a snail’s pace in taking preventative measures. Another issue is that some sites have done nothing at all and remain trapped in the pre-Gamergate paradigm. A third issue is that new Artificial Intelligence (A) gives attackers an edge. Here, AI makes the creation of ‘deep fakes’ child’s play. The sheer speed of technological ‘progress’ and the indifference of many governments and large companies make it hard to defend against determined attackers.

The projects put into action by Anita Sarkeesian and Zoë Quinn are just two of many cyber-feminist initiatives undertaken on the Internet. These initiatives range from apps and webs for complaining about harassment (for example, Take Back The Tech!) to feminist bots to unleash mass responses to trolls. Yet the truth is there is no ‘magic bullet’ for resisting and responding to online violence. Virtual feminist communities have to be flexible and adapt their practices to the circumstances of those suffering one or other kind of male chauvinist violence, whether this takes place online or offline. Speak Up & Stay Safe(r) and Crash Override are two examples of innovative, ingenious solutions for women dwelling in the Internet, helping users create “micro-spheres of action” (Zafra, 2004) and offering support and resources to women suffering one or other form of social violence. Here, both initiatives have done a great deal to change the Law’s lax interpretation of violence perpetrated online as somehow ‘unreal’ despite its clear link to offline violence.

Feminists are stepping into the breach to create archives and communities where platforms refuse to apply their terms of use to all those at risk from online violence (protagonised by the Alt-Right groups mentioned earlier), Such action helps marginalised/oppressed users/communities survive online and become fully-fledged digital citizens, Thus the only way the Internet can safeguard users’ basic rights is to create a web in which the feminist and other progressive causes can flourish free of the scourge of online harassment and threats.

---

6 Carl Benjamin, for example, was expelled from Twitter in 2017 and again in 2019 after hiding behind another made-up name. YouTube demonetised his channel in May 2019 but did not expel him. More recently, it demonetised his second channel ‘Akkad Daily’ in March 2020. Patreon forbade his use of the platform in 2018. The user’s Facebook remains active.

7 This is a technique that uses unsupervised learning algorithms to produce altered but hyper-realistic videos. The approach was used in *vengeance porn* cases to add the faces of famous women to figures in pornographic videos.
BIBLIOGRAPHIC REFERENCES


---

**BIOGRAPHICAL NOTE**

Hanash has a degree in Sociology and Political Sciences, and a Master’s degree in Gender and Equality from Universidad Pablo de Olavide; where she is currently a doctoral student in the Social Sciences programme. Her main lines of research are: digital violence against women; cyber-feminism; feminist resistance strategies against cyber-violence.