

**Maria Qibtia**

Federal Government Fazaia HSS PAF Base Nur Khan, Rawalpindi, Pakistan.

Cite This Article: Qibtia, M. (2026). Cyber Terrorism as Ethical Resistance: A Critical Study of Purity and Dear Cyborgs. *Journal of Social Sciences Research & Policy*. 4 (01), 963-982.

DOI: <https://doi.org/10.71327/jssrp.41.963.982>

ISSN: 3006-6557 (Online)

ISSN: 3006-6549 (Print)

Vol. 4, No. 1 (2026)

Pages: 963-982

Key Words:

Cyberterrorism, Hacktivism, Surveillance
Cyberspatial Tyranny, Internet's
Militarisation, Online Resistance, Privacy

Corresponding Author:**Maria Qibtia**Email: mariqibtia1111@gmail.com**License:**

Abstract: My research investigates the ethicality of cyberterrorism in the form of hacktivism and questions its projection as an anarchic civil disobedience by postulating that cyberterrorism is a politically triggered act of resistance which can be morally justified by considering the ethically motivating factors underlining this act. Through a critical analysis of Eugene Lim's *Dear Cyborgs* and Jonathan Franzen's *Purity*, it contests the arguments of Julie Mehan, C.P. Cumming, Keiran Hardy and George Williams that present cyber-terrorism as a criminal act and a threat. My research focuses on contextualising cyberterrorism as a radical but ethical act of online resistance that rises in response to unjust surveillance capitalism and the internet's militarisation. My research is timely because technological domination, online surveillance and the corresponding elimination of privacy are accelerating. My paper integrates the notions of Julian Assange, Safiya Umoja Noble, and Majid Yar because their theoretical ideas collectively allow me to engage in a rethinking of cyberterrorism's ethicality and to question the phenomenon of mass surveillance that perpetuates a web-based tyranny and its role in making cyberterrorists/hacktivismists ethical subjects. While subverting the negative connotations of cyberterrorism, as my research primarily concludes that the unjust neoliberal power structures and their manifestations justify cyberterrorism as a form of ethical resistance, I highlight the poisonous repercussions of cyberspatial surveillance and the internet's militarisation.

Introduction

Cyberterrorism has been treated as a risk since the beginning of the internet in the early 80s. A number of researches have surfaced in the past which represent cyberterrorism as a threat to the world's socio-political system while completely neglecting its ethical side. The reason behind this angle is the lack of a universal definition of cyberterrorism and the problematic and narrow definitions given by researchers such as Dorothy E. Denning. She defines cyberterrorism as "the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government" (Denning 1). The reason underlying this approach is cyberterrorism's representation as a threat similar to traditional terrorism,

as is debated by Dan Verton in *Black Ice: The Invisible Threat of Cyber-Terror* and Gabriel Weimann in his special report for the US Institute of Peace, "Cyberterrorism: How Real Is the Threat?" Weimann writes about cyberterrorism and its threatening nature in this report by declaring it to be 'very alarming' because of technological advancements. Verton, a former US intelligence officer, on the other hand, has further added to this debate in his book about the criminalisation of cyber terrorists and has written about the potential of cyberterrorism as a threat in detail. Similar to Denning, Kevin Curran et al. define cyberterrorism synonymously with terrorism. They start their article with a definition of terrorism as being "the unlawful use or threatened use of force or violence by a person or an organised group against ... governments, often for ideological or political reasons" and further theorise cyberterrorism with reference to this definition (1-3). They represent cyberterrorism as a form of terrorism and a new form of warfare that happens in cyber space. In some instances, they even refer to hacktivists as 'terrorists' while simply disregarding the possibility of hacktivism or cyberterrorism as an act of ethical resistance. In short, they simply criminalise cyberterrorism without acknowledging its potential as an act of resistance.

Additionally, it is observed that despite the variety of perspectives regarding cyberterrorism, its ethicality is rarely explored in spite of its being a hot topic since the publication of *WikiLeaks*. With this in mind, I have addressed the gap in the existing research on cyberterrorism and have highlighted the ethical side of cyberterrorism in the form of hacktivism, which rises against critical neoliberal infrastructures such as mass surveillance, to contest the preexisting debates that criminalise cyberterrorism.

My research challenges this kind of criminalisation of cyberterrorism as well as the commonly held notion that cyberterrorism is an unethical act and recasts it in terms of ethical resistance. Such resistance has risen against surveillance capitalism that aims to produce regulated subjects through coercion to which cyberspace is no exception, as Safiya Umoja Noble highlights in *Algorithms of Oppression: How Search Engines Reinforce Racism* that discrimination is rooted in the computer code and other artificial intelligence technologies (1). Therefore, I understand cyberterrorism, a subcategory of cybercrime, particularly in its intersection with hacktivism, to be a politically triggered act of civil disobedience which *can* be morally justified. More importantly, this study questions the ways in which powerful institutions and dominant discourses designate such acts as "cyberterrorism" in order to criminalise and delegitimise politically resistant subjects. The designation of an act as cyberterrorism, therefore, is not treated here as a politically neutral classification; rather, it can function as part of the larger struggle over who has the authority to define legitimate and illegitimate forms of resistance.

I have selected two novels for this investigation that are *Dear Cyborgs* by Eugene Lim and *Purity* by Jonathan Franzen. The reason why I selected these two novels is that the characters in these novels attempt online espionage, an act that is termed cyberterrorism, to counter the surveillance and data commodification of the internet. I claim that the characters portrayed as criminals in *Dear Cyborgs* and *Purity* are, in all practicality, ethical subjects working against surveillance capitalism, which is "focused on data extraction rather than the production of new goods, thus generating intense concentrations of power over extraction and threatening core values such as freedom" in cyberspace (Couldry). By ethical subjects, I imply various politically motivated activists who use technological hacking for their hacktivism and constructive civil disobedience, which entails a resistance to power structures that is non-violent. Such civil disobedience aims to bring positive socio-political changes rather than being a threat. Similarly, in these novels multiple resistance strategies, that is, cybercrime in general and cyberterrorism in particular, arise to contest surveillance capitalism. This research, which is delimited to the idea of

cyberterrorism, complicates this notion and represents it as an ethical resistance to neoliberal exploitation both inside and outside cyberspace.

Scholars such as C. P. Cumming, Julie E. Mehan, Keiran Hardy and George Williams have extensively written about cyberterrorism or hacktivism; however, a logical explanation concerning the reasons behind committing such an act and its ethicality is seldom studied. The scarcity of detailed research regarding the ethicality of cyberterrorism invites a thorough study of this phenomenon in order to explain cyberterrorism as a just social and political resistance, and this area having been rarely explored serves as the rationale for my study. Furthermore, depending on the context, cyberterrorism may intersect noticeably with cybercrime, cyberwar and ordinary terrorism. Cyberterrorism, therefore, ends up assimilating multiple controversial definitions, with the most commonly understood form being the intentional use of computers against any government to hack sensitive data and military websites to distribute propaganda material. Thus, I have delimited my study to the hacking aspect of cyberterrorism.

Henceforth, drawing on the notions of Julian Assange, Safiya Umoja Noble, and Majid Yar, I highlight that cyberterrorism is an act of rational resistance. The aforementioned theorists assist me in understanding the workings of power structures in cyberspace as well as the different modes of resistance that exist in cyberspace. Assange's positionality as a hacktivist also elicits the questioning of the negative implications assigned to cyberterrorism, which then rationalises hacktivism. These theorists strengthen my argument and aid in contesting the concept of cyberterrorism as a criminal act which is advocated by Cumming, Mehan, Hardy and Williams. In positioning themselves in opposition to it, they consider cyberterrorism as a weaponising of the Internet which can put states at risk of cyberattacks. I contest these theoretical stances in this research with the help of the notions of Julian Assange, Safiya Umoja Noble, and Majid Yar.

Noble introduces the workings of power structures in cyberspace by highlighting the negative aspects of the internet, such as the reinstatement of racism, discrimination, and sexism, among other things (Noble 1-2). She explains the context for the resistance that is taking place in cyberspace, which has its own power dynamics that are reciprocal to the power structures existing in real life. For instance, through her statement of some basic search results available on the Google search engine, Noble mentions how the internet is specifically targeting Black women and that discrimination is embedded in the computer code because public information online is based on the context of the real, lived experiences (182-183). Therefore, similar to real life, online discrimination and oppression are countered with resistance in cyberspace. Noble's statement of the workings of the online power dynamics justifies the resistance that also takes place online, as she says that when collective efforts or governmental intervention fails to bring any change, then individuals rise with the hope to bring about social change both online and offline (182).

I also take into account some of Assange's own publications, including *Cyberpunks: Freedom and Future of the Internet*, where Assange blames the power dynamics of cyberspace as the cause of cybercrimes. Assange starts his discussion by considering the Internet as the most dangerous facilitator of authoritarianism despite being an emancipatory tool (1). His claim further resonates with Yar's stance about cyber-terrorism, which argues that the totalitarian authority of neoliberal corporate structures dramatises negative depictions of cyberterrorism to justify its accelerating online surveillance and the corresponding elimination of privacy (57). There are laws and regulations that are "intended to protect people's right to privacy, but there are more laws that stifle this right and put their safety and their data's protection at risk", and legalised mass surveillance is a tool of such violation (Kamran). Many

states have “adopted laws affecting online privacy, for example, consumer protection statutes, [and] laws that protect certain categories of PI” (“Internet Privacy Laws Revealed — How Your Personal Information is Protected Online”). However, there are several loopholes in these laws which make it easier for the government to spy on the masses and leave the common people vulnerable. This way of the state that justifies mass surveillance while keeping the power figures out of the surveillance dragnet is, therefore, problematic, and it further makes the accountability of the powerful impossible. Thus, hacktivists like Assange and Snowden rise against such power-based exploitation, and through whistleblowing, they make the accountability of the powerful a possibility. These notions correlate with the texts under study; for instance, Ms Mistletoe in *Dear Cyborgs* resists the power structure by keeping the power figures in the surveillance dragnet and thus makes them accountable for their actions.

Furthermore, Raoul Chiesa et al. also apply the science of “criminal profiling”¹ to the domain of hacking. Chiesa et al. state that hacking is not necessarily a crime because it is distinctive from the real crimes. They even enlist the motives behind the act of hacking (147-159), which includes ‘fighting for freedom’ that justifies the major motive of hacking as defending ‘oneself from violations of the principles that govern the online world, from the attacks of the physical world they consider morally corrupt’ (152). In addition to this, the motives behind the act of hacking also include ‘conflict with authority’, where the hackers think that their privacy is violated by some power structures (153). These motives also include political reasons that can vary from hacktivist to hacktivist (158). In my thesis, the motives behind the actions of resisting actors include mass surveillance and violation of public privacy engaged in by the power structures which lead to their conflict with authority. Their conflict with authority via hacktivism is justified by the unjust actions of the power structures, such as mass surveillance and militarisation of the internet. Moreover, some of the other motives mentioned in the aforementioned book represent hacktivism in a neutral light, that is, neither a justified resistance nor an illegal activity. Hence, Chiesa et al.’s study of the motivations for hacking may not project hacktivism in an ethical light, but it does serve as a justification for proving that in spite of being a radical face of online politics, hacktivism is an act of ethical resistance.

Moreover, the process of resisting through cyberterrorism, to an extent, is an anarchist approach of countering the fatal consequences of mass surveillance, an act that is highly promoted by the capitalist power structures. The rebels rebelling via cyberterrorism can undeniably be termed as anarchists for their rejection of authority. However, such rejection is not unethical but morally justified because the authority being rejected is intensely coercive and promotes the inescapable complicity of the masses with surveillance capitalism, especially in cyberspace. The cyberterrorists do not reject the state in an absolute way; they counter the legitimacy of the existing governmental and the powerful non-governmental institutions by highlighting that those power structures promote the unjust militarisation of the internet, the foundation of which is mass transparency. In other words, cyberterrorism is a rebellion against the power structures, and it stresses the importance of making possible the accountability of those in power and guilty of capitalising on the masses’ information for the sake of profit.

It is only recently in academia that researchers have been trying to represent hacktivism as a defensive position. A few of the existing research, such as the works of Mark G. Milone and Galina Mikhaylova, are dedicated to the ethical considerations of hacktivism while simultaneously condemning specific acts of

¹ Criminal profiling is a technique whereby the probable characteristics of a criminal offender are predicted based on the behaviors exhibited in the commission of a crime. The objective of criminal profiling is to try to clarify why a crime has been committed and what the special traits of the perpetrator are (Chiesa et al. 2-3).

hacktivism as cyberterrorism. These researchers do not rule out the possibility of cyberterrorism as a threat in most cases. Milone even stresses that hacktivists need to be better educated about the importance of national infrastructure such as the critical systems that promote core functions in modern societies, like telecommunications, etc. (1). By doing so, Milone highlights that hacktivism cannot *always* be a threat if people are better informed about the importance of national infrastructure.

Researchers such as Mikhaylova and Milone, in addition to others, define hacktivism as ethical because it aims to bring about a positive socio-political change. These changes include the unveiling of the inner workings of the people in power and their secret diplomatic decisions, in addition to the exposition of mass exploitation such as mass privacy invasions. Milone and Mikhaylova claim that such hacktivism targets governments mostly in mild scenarios, such as the organising of a protest to challenge social norms (Mikhaylova 8). However, their views on hacktivism are limited because they do not explore the more recent purposes of hacktivism. Therefore, my research is timely, as it differs from such past studies and brings into consideration new dimensions of cyberterrorism.

At this point, it can be established that there has been much research done on the potential of cyberterrorism as a threat, but cyberterrorism's ethicality is comparatively less explored even though it has been widely discussed since the publication of *WikiLeaks*. This issue became even more significant due to Assange's most awaited extradition hearing in 2020, which further led me to question the politically established criminality of whistleblowers and hacktivists like Assange.

Exposés by Assange and Snowden: Ethical or Not?

The ongoing legal case against Julian Assange indicting him for cyberterrorism is of particular interest to my work. The recent court hearing of Assange in London makes it compulsory to study and analyse the issue of *WikiLeaks*, which has been criminalised and presented as an act of cyberterrorism², and the politically established criminality of Assange. Deemed to be a criminal for engaging in cyberterrorism under the Espionage Act of 1917, Assange has been incarcerated in HM Prison Belmarsh for unveiling the unjust acts of many American governments and their plans of war and irrational violence against certain countries. This world-renowned 'criminal' was subsequently charged with sexual assaults. Later in April 2019, these cases were mysteriously dropped after his arrest. Assange has been legally imprisoned under psychologically oppressive conditions to this day due to the judge blocking the extradition in the hearing of 2020, hence making this an urgent issue and further making the theorisation of cyberterrorism even more necessary. His politically condemned form of hacktivism leads us to further question the problematic association of criminality with hacktivists like Assange, Snowden and many others who work for the betterment of the masses by disclosing information that affects the public directly.

The socio-political global context of such hacktivists' acts establishes the rationale behind the rise in the phenomenon of cyberterrorism. The prevailing state-centred, coercive and neoliberal power structures, including those governments³ and governmental organisations⁴ that promote mass surveillance and militarisation of the internet (Assange et al. 33), gradually gave birth to the hacktivists' resistance through cyberterrorism in virtual communities. According to Assange, this development means that "we are all living under martial law as far as our communications are concerned; we just can't see the tanks—but they are there" (Assange et al. 33). He further adds that this condition is similar to "having a soldier under your bed" (33). Due to such invasions of privacy in the form of the militarisation and

² Hacktivism is not legally a crime, and when it becomes a crime, it is termed as cyberterrorism. Therefore, Assange's criminalisation is reciprocal to the criminalisation of his acts.

³ Such as the UK, the US, China, Greece, Singapore, and others

⁴ Like America's National Security Agency (NSA), Central Intelligence Agency (CIA), and Federal Bureau of Investigation (FBI)

surveillance of cyberspace, cyber resistance or hacktivism arises to contest them and to aid the masses in making the powerful accountable for their crimes. For instance, Assange's resistance enables people to surveil the actions of those in power. This was seen in *WikiLeaks'* publications of the emails of different Syrian and US political leaders in 2012 in collaboration with the Anonymous group and other hackers that turned the tables on the powerful. The Syria Files did not only disclose the luxurious lifestyle of the Syrian leader, Bashar-al-Assad, and his family while their country faced food shortages and other hardships, but it also exposed Assad taking the reforms he had promised lightly and treating those reforms as an attempt to deflect attention away from the food crisis in Syria. It also revealed Assad's established network of trusted aides who were inclined to report directly to him while bypassing the country's security apparatus. The disclosure of such political events justifies Assange's resistance, as it motivated the public to address these problems with this new knowledge made available to them. Such real-life instances of Assange's hacktivism lead us to justify cyber-terrorism as an ethical act and challenge the opposing negative definitions.

As the editor-in-chief of *WikiLeaks*, Assange also exposed various power abuses on the global level in addition to the irregularities in institutions, both public and private (Burch 227). These include the lack of protective mechanisms in cyberspace and the workings of the surveillance society which threatens the public's privacy and, in the meantime, preserves the secrecy of the powerful ones. Assange claims to liberate information so that it becomes easily accessible to the public while defining mass surveillance as dangerous and unjust (Burch 227). This problem of mass surveillance through the internet is getting worse, developing as a result of its global political complexity, which intends to keep the public under scrutiny while preserving the secrecy of the powerful, thereby making the accountability of the powerful and guilty impossible (Assange et al. 44). Such is the design of mass surveillance. It has been politically justified many times but is nevertheless dangerous. Assange's and multiple other whistleblowers' efforts of revealing various instances of secret wars and human rights abuses in countries like Yemen, Iraq, and Afghanistan, and exposing the presidential participation of these countries in torture and war crimes complicate the hackers' identities as criminals (Radack 326). This ground reality leads us to expose and question the injustice behind their politically established criminality in addition to encouraging the study of the ethicality of cyberterrorism.

In addition to Assange, Snowden's motivations for leaking classified documents regarding mass surveillance programmes also allow us to re-evaluate the counterperspective to the ethicality of cyberterrorism. His first encounter with the mechanism and machinery of mass surveillance was with China's surveillance of private communications, which, according to him, was impressive but totalitarian nonetheless (Snowden 165). Snowden further claims that agencies such as the CIA⁵ and NSA⁶, with the consent of the government, always scrutinise the privacy of people, guilty and innocent alike. Their surveillance works like a "one-way mirror", which is usually a transparent glass placed between the powerful and the masses through which the public "appears in plain view" to the powerful, while the glass being "opaque" on the public's side is the reason why "the watchers went unseen" (Gellman 1). Thus, because of such problematic conduct of surveillance that only works one way, the hierarchies were formed online. These hierarchies hold the surveilling authority at the top, that is the government and governmental organisations, and the surveilled subjects at the bottom, that is, the general public. Such mass surveillance exploits the sensitive data of the people who are "believed to be potentially

⁵ The Central Intelligence Agency is a civilian foreign intelligence service of the United States, tasked with gathering, processing, and analysing national security information from around the world, primarily through the use of human intelligence.

⁶ The National Security Agency is a national-level intelligence agency of the United States Department of Defence, under the authority of the Director of National Intelligence.

associated with" the target of the agency when caught in the surveillance dragnet, and it becomes a source of fun among the intelligence officers (Snowden 269-270). Snowden mentions the officers commenting on sensitive photos of those women caught in the surveillance dragnet because of their association with the target. The privacy invasion of such innocent people, especially women, is what makes the secret surveillance truly unethical and unjustified. These people who were associated with the target of the agency were not guilty of any violations of the law; therefore, their surveillance was problematic, and hence, it makes Snowden an ethical subject and justifies his position of resistance for bringing to light governmental organizations like the CIA's and NSA's unethical penetration into the privacy of the innocent and unassuming public. Hence, Snowden's hacktivism helps in questioning the governmental officers' acts of making a spectacle of the innocent people's lives and thus justifies Snowden's hacktivism. This situational reality therefore makes it necessary for us to question the power structures and analyse hacktivism through an ethical lens.

More than once have hacktivists like Snowden exposed the unethicity behind mass surveillance and lifted the veil of secrecy that saves the powerful from scrutiny and thus provided us with information that is needed for justice and accountability. Consequently, it becomes necessary to question the US government's efforts towards criminalising both journalism and hacktivism by introducing a counter perspective regarding its ethicality, and literary texts can provide such a site of analysis as well as experiment with the possibilities that such circumstances generate via fictional representations.

Hacktivism in *Purity* and *Dear Cyborgs*

My foregrounding of the concept of 'cyberterrorism as ethical resistance' relies on studying resistance strategies and resistance identities forged against online power dynamics. This concept is illuminated in the selected novels *Purity* and *Dear Cyborgs*, where various characters utilise illegal techniques such as cyberterrorism, all the while intending to bring about some positive socio-political transformation. The resistance of these characters takes the form of anarchism, which serves as their ethical framework. Therefore, I am subverting anarchism's negative connotations in this research in addition to those of cyber-terrorism. The characters in these novels carry a certain resemblance to Assange, who, despite being labelled a criminal, positions himself as an ethical subject by challenging the multinational corporations of the neoliberal state, the American exceptionalist drive and the notion of "don't be evil" (Assange 35). Assange's cyber criminality forges a new concept of the ethicality of crime and is, therefore, highly pertinent to this research.

Similarly, both novels depict cyberterrorism as a rational and ethical act. Ms Mistletoe in *Dear Cyborgs* and Andreas Wolf and Purity, aka Pip in *Purity* create resistance identities to fight unbearable socio-political oppression. Ms Mistletoe is portrayed as a villain and a criminal in the world of superheroes employed by the government to fight against her. This criminalisation of cyber terrorists like Ms Mistletoe shows the power structures' stance towards cyberterrorism, which disregards the ethical reasons behind the act and its function as resistance. Hence, the context of her criminal acts, which revolves around revealing the unethical actions of the powerful and making them accountable for their crimes, rationalises her decisions to rise against the government and resist through cyberterrorism.

Comparably, in *Purity*, Andreas Wolf built the Sunlight Project, a fictional competitor to *WikiLeaks*, to spy through computers on the critical infrastructures of multinational corporations as an act of resistance, and Pip helps him in one of the activities of this project. The character of Andreas Wolf parallels Assange's. Wolf becomes an internet celebrity while being a wanted man at the same time in most countries for revealing confidential state-owned information to the public, thus leading us to problematise Wolf's identity. His state-formulated criminalisation shows his proximity to the disclosure

of the truth about the powerful and making them accountable for their deeds. His resistance to the global power structures threatens the status of the powerful while doing a service for the betterment of the masses. In short, these characters turn to hacktivism in a similar way to Assange and Snowden, which Assange considers to be a clever solution to severe problems such as exploitation of the weak (Dreyfus and Assange xiv).

Problematising cyberterrorism and its criminalisation also necessitates a close observation of its depiction in the existing literary works. Over the past three decades, as stated in the introduction, cyberterrorism has been seen by many as a threat. They represent cyberterrorism as an illegal act while overlooking the possibility of an illegal act functioning as an act of resistance that arises in response to oppressive power regimes, as was done by Assange's *WikiLeaks*. Henceforth, it is observed that cyberterrorism has been mostly studied as an unpatriotic and violent act while neglecting the reasons behind this act of resistance altogether. Considering the ethical reasons behind this act, I suggest that cyberterrorism is a form of resistance rather than a threat. The texts that I have selected as sites of analysis further substantiate my argument and represent cyberterrorism in an ethical light.

Research Objectives and Questions

The discussion above provides the grounds for formulating the research aims of the present study, which is closely aligned with its central research questions. Accordingly, this study aims to highlight surveillance capitalism and the militarisation of cyberspace as manifestations of neoliberal power dynamics and the potential of cyberterrorism as an ethical form of resistance against those power dynamics as presented in the selected novels. In line with this aim, the study asks: How do surveillance capitalism and the militarisation of cyberspace rise as manifestations of neoliberal power dynamics? And how do the selected novels reveal the potential of cyberterrorism as ethical resistance against surveillance capitalism and militarisation of the internet? I analyze the selected novels by keeping in mind the positionality of real-life hacktivists such as Assange and Snowden and compare it to the hacktivists in the selected novels to foreground my claim.

Surveillance Capitalism v/s Cyberterrorism in *Dear Cyborgs* and *Purity*

The main questions that govern my research pertain to surveillance capitalism and the militarisation of cyberspace as manifestations of neoliberal power dynamics while operating in cyberspace and the potential of cyberterrorism as ethical resistance against such manifestations. Therefore, in this research my focus is two-pronged. First, I explore the workings of the internet and their power dynamics through the analysis of the selected novels, *Dear Cyborgs* and *Purity*, with the assistance of the relevant theoretical approaches. Secondly, while highlighting the exploitation at the hands of online power structures, I foreground hacktivism as ethical by rethinking it as a solution to these injustices.

More importantly, these notions are flagged in *Purity* and *Dear Cyborgs* where the characters utilise illegal techniques that fall within the circumference of cyberterrorism while intending to bring about some positive socio-political transformation. Andreas Wolf in *Purity* and Ms Mistleto in *Dear Cyborgs* carry a certain resemblance to Assange, who, despite being labelled a criminal, positions himself as an ethical subject. Assange's cybercriminality forges a new concept of the ethicality of crime, and in this research, I use this concept to analyse the ethicality of cyberterrorism in the form of hacktivism through the examples of Andreas Wolf and Ms Mistleto, who are engaged in similar forms of resistance which, in certain circumstances, make the ethical conception of cybercrime highly pertinent to this research.

My research from this point onwards clearly shows that cyberterrorism is not a vicious threat to the society and thus challenges the views of those researchers who slight the possibility of resistance enacted via cyberterrorism, that is, a resistance that rises in response to oppressive power regimes and

human rights abuses, political blunders and power abuses generated on a global level. Finding anchorage in the aforementioned ethical intentions underlining the apparent unethicity of cyberterrorism, I develop my argument with the help of pertinent examples from the selected texts.

Cyberterrorism: an Effective Ploy against Surveillance Capitalism

The novel, *Purity*, explicitly engages with the issue of surveillance capitalism in cyberspace and presents cyberterrorism as a probable solution to this issue. The main character is a working-class American named Pip. Due to a substantial student loan debt, she works minimum-wage jobs while residing temporarily in a house that is at risk of foreclosure (Franzen 40). Franzen makes many subtle references to the character of Charles Dickens' Pip in *Great Expectations* through Purity aka Pip's problematic relationship with her mother, her absent father and the coincidental and melodramatic plot twists regarding the identity of her father. Franzen's Pip also aids Andreas Wolf, a criminal with ethical intentions, in his cause just like Dickens' Pip had once helped Magwitch, an escaped convict with ethical intentions.

Franzen's Pip, along with her roommates, used to shelter German travellers in Oakland, and one of them introduces Pip to Andreas Wolf, a cyberterrorist and a figure reminiscent of Julian Assange. Wolf runs the 'Sunlight Project', which is an international organisation that reveals information regarding public figures, political figures, and large corporations. Pip thinks of using the Sunlight Project to locate her father when she realises its technological scope and leaves for Bolivia to work at its headquarters. She starts to live among people with secrets. In fact, for the greater part of the novel, she tries to clarify the motives of those around her. Working under Andreas is a challenging task for Pip, but her interest in working on the Sunlight Project is prompted due to the refusal of her mother to provide any information about her biological father's identity.

Pip's father, Tom Aberant, for whom she later works without being aware of his identity, meets Andreas in Berlin and helps him in burying a corpse. Subsequently, Andreas uses his technology to uncover the identity of Tom's vanished ex-wife. In doing so, he comes to know that Tom was Pip's biological father and therefore sends her to spy on Tom's journalism in an effort to engage in counter-blackmail. Secrecy and its consequences, thus, are integral parts of the plot. In *Purity*, the immediate social crisis is concerned with the promise of democratising the internet. Andreas Wolf's project is devoted to transparency and making the internet a platform where accountability is possible and justice prevails. People are allowed to express their political inclinations and are able to protest for a just cause. This focus on democratising the internet enables me to read this novel in alignment with *Dear Cyborgs*, whose characters also use the internet as a platform to make the powerful accountable for their wrongdoings and make the internet a safe place for the masses.

Interlacing comic-book villains such as Ms Mistleto with cultural critique, *Dear Cyborgs* is a novel about the power play between key political figures and rebels in addition to an exploration of the notion of protest through creative arts. It interweaves detective pulp fiction, dissident philosophy, and Hollywood chase scenes in a dream-like manner. By cyborgs, Lim refers to ordinary human beings who have become extremely dependent on technology since its advent and made it possible for the powerful to control the masses through technological devices and the internet. Lim, throughout the novel, tries to educate the readers about their oppression and the technological control of the powerful and therefore titles the novel as *Dear Cyborgs*. This novel consists of three storylines; one storyline tracks a series of letters addressed to *Dear Cyborgs* by a mysterious sender. This is similar to how the novel works, that is, as a letter addressed to the reader. Another storyline is about the memories of an unnamed man and his childhood friend, Vu. They become friends in a small Midwestern town due to their outcast status, a

consequence of their being the only two Korean boys in town, and a mutual love of comic books. The final storyline of *Dear Cyborgs* can be summed up in one of Vu's dialogues at the end of the novel:

Superheroes going out to lunch, complaining to their therapists, unsure about their parenting styles. A chase scene where the driver and his passenger, while making split-second decisions, talk about different forms of resistance to power. A murder mystery where the detective receives a call at the crime scene from her father and she tells him her theories about the history of suicide protests around the world, analyses of madness and megalomania versus desperate agency, and the dangers of aestheticizing violence (160).

This storyline is about a villain and a team of superheroic characters who, through a series of linked monologues, explore the narratives of resistance-protest art, pyromaniacal militants, eco-terrorists, and occupy-squatters, as well as about protestors influencing the cold demands of contemporary capitalism, which makes the rich richer and the poor poorer. It is about another timeline or an alternate universe in which a group of superheroes — who have special abilities and choose to work with the US government to catch any viable threats to it — contemplate contemporary American society during their free time. When they are not on black-op missions or rescuing hostages, they hold detailed discussions on the subject of the inescapable grip of market economics and different forms of resistance to manipulative power. All of the scenes mentioned in the quote above are those stories that become the subject of discussions among the superheroes. These discussions are extremely vital to my research as they explain the workings of power dynamics in cyberspace and also the reasons behind various forms of illegal resistance such as cyberterrorism. In one such discussion about the inescapable clutches of capitalism, they talk about the NSA's mass surveillance in cyberspace:

These [NSA] computers held the phone and internet usage logs of all those citizens who were terrorist suspects as well as the phone and internet usage logs of all those citizens who were not terrorist suspects (Lim 17).

What this quote indicates is that in the novel's world, powerful governmental and non-governmental organizations have introduced mass surveillance to militarise the internet and capitalize on the data of the masses for profit, which threatens the public's privacy as well, thereby revealing mass surveillance as dangerous and unjust (Burch 227). Since more and more people are using online platforms, the social media platforms are treated as data mines. Such "data explosion that has put privacy and security in the spotlight will accelerate" with time due to our dependency on technology (Kerry). This problem of mass surveillance through the internet is becoming bad and will become even worse in the real world as it intends to keep the public under scrutiny while preserving the secrecy of the powerful (Assange et al. 44). In this process, these powerful organizations do not only target those suspected of global terrorism but also innocent citizens.

Dear Cyborgs is a combination of many mini-narratives based on the aforementioned subjects. These are cleverly embedded in its two main storylines through monologues. These monologues are delivered by characters that possess super heroic abilities, and the vigilante, Ms Mistleto, indirectly rationalizes these cyberterrorist acts as ethical resistance. For instance, in the first monologue of Ms Mistleto, she justifies her position as a hacktivist by explaining the reasons behind Occupy Wall Street and many other protests in general. Occupy Wall Street was one of the major protests against economic inequality that began in Zuccotti Park, New York City, in the Wall Street financial district. It gave rise to other wider Occupy movements in the US and other countries. *Dear Cyborgs*, These protests are mentioned in relation to Ms Mistleto's resistance, which justifies her choices. She would rather be called a cyberterrorist than have any "complicity to injustice" just as her fellow protesters were ready to risk

their freedom for justice (Lim 18-21). Ms Mistleto clearly mentions the intentions behind these protests in one of her monologues, which included “job losses, wage stagnation, arrests, intimidation by hired thugs, and the increasing persecution of workers” (19).

Ms Mistleto’s monologues, in addition to the monologues of the other superheroes, expose the underlying theme of the novel, that is, protest. In these monologues, the characters discuss the philosophy behind the protests which subtly reveals their ineffectiveness and the powerlessness of the protestors. Ms Mistleto, in one of her soliloquies, recalls her discussion with a protestor who defines the phenomenon of protest as “a spoiled kid having a tantrum ... It’s annoying for the adults who have to respond, but they can’t really take the tantrum very seriously” (20). She acknowledges the failure of the protests as she continues her discussion with the protestors in Zuccotti Park. She forms her own explanation of the phenomenon of protest and considers it “in part an expression of hope and in parts an expression of guilt” (21). For her, it is an expression of hope because a protestor protests for an ideal state of a society to get rid of all evils, including capitalism and its various manifestations, which, in spite of its being impossible to achieve, can save people from “complicity to injustice” (21). On the other hand, Ms Mistleto sees it as an expression of guilt because, similar to a “buyer’s remorse”, protest is “like a regret that comes after the purchase of something you don’t really need and which isn’t after all you’d wanted. It is like asking people to wake up to the fact that their desires have been manufactured, that the lives they are leading are modeled after flawed received ideas” (21). In this remorse, the protestor hides the guilt which is based on the knowledge that “the entire social contract is contaminated, tainted, since it requires the hard labor of the unfortunate ... and even more subtly, an embedded faith in the eventual good of selfishness and greed” which forms the base of capitalism (Lim 21). Since the base of capitalism is founded on greed, the manifestations of neoliberal capitalism, such as surveillance capitalism, are problematic, as they are a threat to the masses, disguised as welfare strategies for them by the government. Surveillance capitalism reinforces hegemonic narratives and exploits its users (Noble 179). Therefore, to challenge such governmental exploitations, people turn to a method of protest which is often considered “a reactionary or collaborative tactic” but nonetheless is the only legal and “possible defiance” (Lim 8).

However, this possible defiance rarely brings forth any real change, but still, after a certain amount of effort and loss, “cosmetic or otherwise deceptive reforms will be enacted — but these usually just better camouflage for an otherwise unchanged apparatus” (Lim 23). For instance, the Syrian leader, Bashar Al Asad once used the reforms he promised to deflect attention away from the food crisis in Syria. So the protestors appear to be a part of a meaningless and useless phenomenon. At the risk of their lives, they demand positive change, fair elections and aim to take the best from their imperfect system (Franzen 151). For instance, Pip’s friend, Stephen, lives cash-free to passively protest the immiseration of billions of people (Lim 39). Stephen hopes to bring positive change through such meaningless ways of protesting the increasing economic impoverishment but fails to do so (15).

In juxtaposition with *Dear Cyborgs*, the futility of the regular peaceful protest can be further explained through *Purity* as Andreas also bears witness to the meaninglessness of the protest when he, on a usual basis, starts going outside the Stasi⁷ compound and mingles with the protestors. He always sees the same faces of men and women “who’d been interrogated and imprisoned for bad reasons and bore adamant grudges against the ministry” (Franzen 154). But to no avail, these protestors gather almost every day in front of the compound, but they are hardly noticed by the Stasi because in their eyes they are harmless and rarely have had anything happen in the past due to their protest. People were still

⁷ The Stasi was the Ministry for State Security of the German Democratic Republic (East Germany, GDR) from 1950 to 1990

being imprisoned and wronged; for instance, one of the protestors tells Andreas that he was imprisoned for defending his “female classmate from the sexual advances of the son of a Stasi commander’s son” (Franzen 154). The sexual predator remained free while the saviour was imprisoned and criminalised with dubious charges.

The selected novels justify hacktivism as a viable form of protest by explaining the failure of peaceful protests and defining peaceful protest as an act of minimal participation where one only escapes complacency by providing a reflection on the geopolitical events without “going into heroics” (Lim 8). They present regular protest as a futile and “vaporous defiance” and introduce hacktivism as the only possible form of resistance, which is like “going into heroics” (Lim 8). These novels have many indirect references to cyberterrorism/hacktivism being a viable answer to the unending socio-political problems. Such references also include the monologues which explain the futility and subtlety of protest while demanding real action which brings real change. For instance, Ms Mistelto’s explanation of the ineffectiveness of protest indirectly justifies her choice of hacktivism (Lim 18-23). One of her fellow protestors describes the protest as “a spoiled kid having a tantrum...they [the authorities] can’t really take the tantrum very seriously” (20). Hence, these subtle references to the failure of regular protests in bringing about any positive results in favour of the causes of the protests validate Ms Mistelto’s and Andreas Wolf’s turning to cyberterrorism with the intention of bringing about some genuine change in the failing capitalist society of America and Germany. This approach challenges the dramatised negative depictions of cyberterrorism as a criminal act which aims to coerce any government at the cost of violence (Yar 57).

Furthermore, the discussions mentioned in Ms Mistelto’s monologues justify taking hacktivism as a form of protest which is often considered immoral and a threat to various aspects of critical infrastructure such as national security (Mehan 54). According to Ms Mistelto, even if one is protesting through extreme means such as cyberterrorism, “for the protestor, the protest makes a moral world in which she can abide” (Lim 24). So, she regards cyberterrorism/hacktivism as a form of protest which can actually bring forth some tangible positive change, unlike other forms of active protests that she has participated in in the past. Through hacktivism, she challenges the neoliberal corporate structures which provide a rigid understanding of cyberterrorism to justify its accelerating online surveillance (Yar 57).

I refer to these monologues in *Dear Cyborgs* more often because they reveal vital information about the characters and different forms of protests and resistance which indirectly justify Ms Mistelto’s choice of using cyberterrorism to bring about a positive social change and help in supporting my argument. Through these monologues, as the novel develops, the futility of protests and the efficacy of hacktivism are further highlighted. For instance, in one of these soliloquies, Lim explores the use of art as a mode of protest against certain aspects of capitalism such as wage stagnation in addition to the art market’s capitalism. This is illustrated through Ursula, an artist acquaintance of Frank Exit, who is one of the super heroes, who once made a painting called ‘*Ursula’s Curse*’, which was just a simple statement written in white against a plain black background. It read:

This painting cannot be bought or sold for more than the total wages of six months full-time employment at the minimum wage as determined by the state of New York. If this painting should be sold for greater than this amount, may both the buyer and seller be considered shit by the entire world and by themselves, and may they spend the afterlife as sad and angry and hungry and hopeless as poverty makes (29).

This “curse” was later put on all her works. It was deemed an attempt to fight the art market’s capitalism, which ended in bitter criticism for the artist but she did not let the art market capitalise on

her work as they normally would. Through this artistic piece, the artist resisted the problem of wage stagnation in America in addition to the capitalism of the art market; however, it failed to bring about any intended changes in the system. Thus, no matter what sort of peaceful protest the people turned to in order to resist the unfair handlings of capitalism, they failed intensely and incurred its greater wrath. Additionally, non-artistic people used different forms of resistance, such as “the native people, the immigrants, the various rent boys and sex workers, the working poor” (139) who were left behind, while the rest of the world made billions through technological creations and their use. They resisted technological oppression through aggression; they started to burn things when their struggle was neglected. They were not paid any attention after their non-violent protest, as “at first these alienated locals just muttered their complaints or vandalized” (139). So “a group of people, snapped” and “it became more serious” as they turned to violence because it seemed to be their only way to become visible to the elitist American population. These ‘pyromaniacal’ militants hijacked and blew up special corporate vehicles like the Google, *Facebook*, Apple, and eBay buses. However, their violent efforts went in vain as well, a fact that became poignantly evident as one of these rioters spray-painted the startling sentence “it is easier to imagine the end of the world than the end of capitalism” on one of the buses they had hijacked (141).

Furthermore, the superheroes would also devise ways to resist and influence the cold demands of contemporary capitalism, such as the prioritisation of profit over human health. In one of their sittings, they came to the conclusion that the strategy of parasitism, a way to fight a capitalist franchise by buying the cheapest beverage and occupying a table for hours to slow the business, is one of the best possible ways to rebel against a capitalist food chain which produces “environmentally corrosive food” (Franzen 128-132). This method is the most passive and legal form of protest, but it still fails to bring about any major change in the capitalist American system. This failure yet again justifies Ms Mistleto’s decision of becoming a cyberterrorist.

The Ethicality of Cyberterrorism: Contesting Internet Militarisation and Mass Surveillance via *Dear Cyborgs and Purity*

The expansion of surveillance into digital neighbourhoods⁸, that is, those geolocations where social media is used more often than others, has an extremely political flavour which promotes capitalism (Anselin & Williams 308). The access to the data of the masses, which is extracted from social media platforms such as *Facebook*, is commodified and sold for profit. Many technological giants, including Mark Zuckerberg, the founder of *Facebook*, sold access to the data of their platform’s users to tech firms such as Amazon for targeted advertisement, especially in America. Research showed that sixty-three per cent of *Facebook*’s earnings come from such targeted advertisement (Shapiro). Using such electronic surveillance as a tool of power depends on collecting the data of the masses to either control them or to capitalise on it for financial goals because “information is the oxygen of control” and “secrecy and surveillance, intertwined, define its flows” with its value depending on catching its targets unawares (Gellman 5).

This unaware state of the targets is vital to the process of surveillance because forewarning a person of interest for the sake of accountability or even the general public for the purpose of profit or control can turn the public into self-surveilling subjects, and this is how governmental and non-governmental organisations like the NSA justify their mass surveillance. The nonconsensual surveillance of the innocent is problematic, but that of the powerful and guilty can be effective in bringing accountability.

⁸ Luc Anselin & Sarah Williams in their sociological study define this term in connection with the increasing surveillance in the contemporary world. They especially refer to the areas where social media use is higher than other areas as digital neighborhoods.

So it is vital to Wolf's as well as Ms. Mistleto's hacktivism to use the data of the powerful people to make them accountable for their injustices while they are oblivious to being surveilled, and their information gradually becomes a way of controlling them and perhaps to introduce improved political policies regarding accountability of the guilty. These hacktivists use surveillance as a tool of the powerful people on the powerful people. Ms Mistleto hacks sensitive and critical information of certain politicians, including the President of America, several members of Congress and two Supreme Court justices, to highlight their incompetence (Lim 88-89). She uses the information available on their personal emails and drives as the tool of control while they are incognisant of being watched.

In like manner, Wolf compromises the emails of certain corporate heads to highlight their culpability in sexual harassment or oppression of women in general while the unsuspecting targets are unaware of being surveilled (Franzen 58). Hacktivists like Wolf and Ms Mistleto turn the "one-way mirror" of surveillance towards the powerful for the sake of accountability (Gellman 1). However, hackers and hacktivists disrupt hierarchies which uphold the surveilling authority, that is, the government, at the top and the surveilled subjects, that is, the masses, at the bottom, by their counter-surveillance. They surveil the surveilling authority and bring accountability for their crimes and moral misconduct and are thus termed 'cyberterrorists' for their actions. Such labelling facilitates the powerful in demonizing the strategies that expose them. However, the intentions and motivations behind the cyberterrorism of Wolf and Ms Mistleto justify their crime as being an ethical act.

Andreas Wolf and Ms Mistleto, like Julian Assange and Edward Snowden, work for the public through their hacktivism. Their intentions, which underlie their illegal actions parallel the motivations of real-life hacktivists such as Snowden, who, under the alias of 'Verax', confessed that his:

[S]ole purpose is to inform the public as to that which is done in their name and that which is done against them. The U.S. government, in conspiracy with client states, chiefest among them the Five eyes — the United Kingdom, Canada, Australia, and New Zealand — have inflicted upon the world a system of secret, pervasive surveillance from which there is no refuge. They protect their domestic systems from the oversight of citizenry through classification and lies, and shield themselves from outrage in the event of leaks by overemphasizing limited protections they choose to grant the governed. I tell you from experience that these protections can be stripped away in an instant. (Gellman 30-31)

Snowden highlights in his confession the problematic side of mass surveillance in addition to offering a clarification of his intentions which indirectly justifies his choice of action against such manipulations. He points towards the preservation of the secrecy of the surveilling authority and the vulnerability of the public who are always under inescapable surveillance, which can be challenged by surveilling the authority in return. Therefore, to counter mass surveillance and surveillance capitalism, in a way similar to Snowden, Wolf and Ms. Mistleto turned the tables on the powerful and stripped them of their protections via hacktivism. Wolf revealed the misconduct of the federal government through their settlement with corporate structures such as the Bank of Relentless Pursuit by hacking into their official emails and exposing their patterns of misrepresentation, deceit and theft which they used to make profit (47). The complacent attitude of the federal government regarding these injustices on the part of the bank cast them in an extremely unflattering light. This Complacency towards injustices is a representation of the federal government's being a part of the problem, as all the while it evades accountability. For this reason, mass protests fail to bring about any change or make anyone accountable for the injustices done to the masses which ultimately lead to the birth of extreme solutions such as cyberterrorism.

I do understand that cyberterrorism in the form of hacktivism may not always be the right answer to matters of exploitation, but sometimes it becomes the only real solution to the overwhelming problems being introduced by the failing system of our contemporary society. For this reason, it is basically a last resort for hacktivists like Wolf and Ms Mistleto. Ms Mistleto started off as a protestor but gradually, through a process of individuation, which I will explain in detail in the next chapter, became a cyberterrorist. Her extreme actions were caused by very noble intentions, as her demands show that she, like the real-life hacktivists Snowden and Assange, worked for the public even if it led to her being criminalised. Her demands included "the adoption of a single-payer universal health care system, mandatory carbon caps, nuclear disarmament, paid yearlong parental leave, and tax on all securities transactions" (Lim 49).

Wolf, on the other hand, became a hacktivist by chance as he needed to get rid of the files the Stasi had on him which probably showed his connection to the murder of a paedophile Stasi officer. His committing of this murder can be backed with the ethical intention of saving a teenaged girl, Annagret, from that pedophilic officer who was her stepfather. Wolf later on turned to hacktivism after becoming a media sensation by spilling the truth on camera about the Stasi organisation and the government. He had memorably said, "I'm not here to work *with*, I'm here to work *against*. This is a country of festering secrets and toxic lies. Only the strongest of the sunlight will disinfect it!" which later became the slogan of his project (Franzen 167, emphasis in original).

Wolf's identity as a hacktivist is perhaps more complicated than Ms Mistleto's, and his intentions, initially, were not as pure as hers; however, through the Sunlight Project, he was able to highlight many social issues, including sexism, as he made some corporate organisations, like the Bank of Relentless Pursuit, accountable for their injustices. So in other words, hacktivists like Wolf and Ms Mistleto liberate information to make it easily accessible to the public while revealing the unjust and possibly dangerous aspects of mass surveillance, which is similar to "having a soldier under your bed" (Assange et al. 33). Hence, such ethical intentions of hacktivists behind conducting an illegal act, that is cyberterrorism, justify their choice of resistance. The invasion of the privacy of the general public was problematic for them, and hacktivism seemed to be the only way for them to disrupt the unfair authority of the government and other power structures that promote electronic surveillance to militarise the internet and use surveillance capitalism to capitalise on the people and coerce them. Their hacktivism, in short, was a reaction to mass surveillance and surveillance capitalism which targeted the guilty and innocent alike (Snowden 269-270). Whether it is the data that Andreas Wolf collected from the German and the US governments' databases or the information stored by the NSA about the innocent as well as the guilty (Lim 17), both instances point towards the notion of mass surveillance as more of a problem than a solution to terrorism. These novels depict that through surveillance capitalism, the people in power violate the privacy of the masses by making it look like an ideal solution for bringing peace. However, the ground reality is that the collection of personal data is done in the name of the commercialisation of the internet⁹ which is another form of privacy invasion. Such commercialisation aims to produce personalised advertisements on the screens of the common people to make them "buy, at just the right moment, just the right brand of" the things they think they need (Lim 79).

Through such targeted advertisement, the capitalist industry can sell us anything, including things which are hazardous either to the environment and/or to our health, such as the products of food outlets like McDonald's, Burger King or Wendy's. Their attractive advertisements on the internet pull the people towards their outlets, and the people, in full consciousness, pay for their "mass produced,

⁹ Commercialization of the internet refers to managing online services for financial gain.

environmentally corrosive food” just because it brings them temporary comfort (Lim 128). Such dangers of surveillance capitalism and mass surveillance find parallels with real-life events, as *Facebook* has also sold the data of millions of their users for such targeted advertisement for capitalist gain. An example is the 2018 *Facebook*-Cambridge Analytica data scandal (*The Great Hack*). The company called Cambridge Analytica collected the personal data of tens of millions of *Facebook* users in order to target them in political campaigns which disrupted the UK’s and US’ politics. It purportedly helped Trump win the US election, which would have otherwise been highly unlikely. Additionally, it became one of the forces which promoted Brexit. So *Facebook*, like numerous other social media platforms, is only apparently free; in reality it is a money-making app which capitalises on our data; therefore, such commercialisation of the internet is termed as a form of privacy invasion.

Lim clearly represents this side of the internet in *Dear Cyborgs* and also highlights how the rich and the powerful are comparatively safe from such privacy invasions, as they are the ones doing the privacy invasions and profiling the general public (78-79). Similarly, Franzen further throws some light on this corrupt aspect of the internet, especially in terms of transparency, by highlighting how Wolf spent many years as an advocate for the transparency of the powerful, but as soon as he became one of the powerful people, his priorities shifted, and he cleverly tried to stay out of the transparency dragnet to protect his image in a manner similar to that of the people he had targeted earlier. In an email exchange to Pip he discloses that “public figures must be especially careful” when “revealing anything shameful to anyone” because that way they “run the risk of exposure, censure, mockery” (Franzen 65). Hence, the irony is that Wolf, through his hacktivism, revealed the shameful injustices of other powerful people for their accountability, but when it comes to Wolf himself, then he is particularly careful in sharing anything ‘shameful’ that he had done in the past. Therefore, as an advocate of transparency of the powerful, Wolf himself is unfair when it comes to his own privacy in a similar way to the people he targeted through his hacktivism. Thus indirectly, through Wolf’s corruption after becoming powerful, Franzen reveals the problematic side of transparency and shows that mass surveillance is a key to absolute control more than it is a solution to any of our existing problems, which makes it difficult to justify this manifestation of neoliberalism.

Furthermore, surveillance capitalism eventually became a tool of ultimate control for the powerful, through which it is not only governments but also powerful online platforms like *Facebook* that invade the privacy of the masses. Eventually resistance in the form of hacktivism challenges such exploitations. At this juncture, in order to further carry my argument on to the point where I explain how cyberterrorism challenges surveillance capitalism through ethical resistance.

Surveillance Capitalism and the Internet

The problem of mass surveillance is becoming worse as it intends to keep the public under scrutiny while preserving the secrecy of the powerful (Assange et al. 44). It is often used to make a profit. Its expansion into digital neighbourhoods is even more political as it promotes capitalism (Anselin & Williams 308). Such surveillance capitalism reinforces hegemonic narratives and exploits its users (Noble 179). With mass surveillance, the capitalist corporate heads have made online social life open to data collection and data processing. They either control the masses or capitalise on their data for financial goals because “information is the oxygen of control” and “secrecy and surveillance, intertwined, define its flows” (Gellman 5). Therefore, to contest such online exploitation through surveillance and the public’s inescapable complicity with it, cyberterrorism rises as resistance when every other legal tactic of protest fails to be an effective tool in bringing about any positive change. Therefore, I have highlighted cyberterrorism as an act that challenges the unjust powerful governmental and non-

governmental organisations that have introduced mass surveillance to militarise the internet and capitalise on the data of the masses. The selected novels aid in justifying cyberterrorism and hacktivism as a viable form of protest by explaining the futility of peaceful protests and indirectly referring to cyberterrorism as a practical answer to the unending socio-political problems. They present regular protest as a “vaporious defiance” and introduce hacktivism as the only effective form of rebelliousness (Lim 8).

Furthermore, my research has shown that Assange’s resistance corresponds to the resistance portrayed in the selected novels which further unravels the ethicality of his actions. For instance, in Franzen’s *Purity*, the character of Andreas Wolf carries a marked resemblance to Julian Assange and ‘The Sunlight Project’ that he runs is almost also similar to *WikiLeaks*. Franzen has even compared this fictitious character of Wolf to his hacktivist rival, namely Assange, in *Purity* (47). Eugene Lim’s *Dear Cyborgs* also highlights the internet-based use of global political praxis by foregrounding how the transparency offered by digital platforms is selective and manipulated by the people in power. For instance, the private emails of a politician are much more different and problematic than what is publicly shared on their social media. Some of the covert internet activities of politicians are revealed by Ms Mistleto when she hacks into their computers (88). In the process of bringing accountability to the powerful figures, she is represented as the head of a terrorist group. So, it can be deduced that the novels help in justifying such ‘unethical’ actions by highlighting the underlying ethical intentions of the hacktivists. My analysis demonstrates that the illegal Resistance portrayed in the novels is justified by the motives underlying it. They justify my argument, as these fictional events parallel the real-life instances of hacktivism. For instance, Google, in 2011, worked with *SayNow* and *Twitter* engineers to provide a route of communication for the Egyptian people in response to the governmental internet blackout that hindered their communication with the world at large. Such an act of hacktivism was in effect an act of resistance against the injustice sanctioned by the Egyptian government.

Additionally, I do understand that cyberterrorism in the form of hacktivism may not always be the right answer to the matters of exploitation, but sometimes it becomes the only possible solution. For this reason, it is basically a last resort for hacktivists like Wolf and Ms Mistleto. These characters in the novels serve the public through their hacktivism. The intentions which underlie their illegal actions parallelise the motivations of real-life hacktivists. Their extreme actions are backed by tremendously noble intentions, as in a similar manner to the real-life hacktivists Snowden and Assange, they worked for the public even if it led to their being criminalised. Considering that cyberterrorism is extremely political, I understand that it may not be the right approach to rebel, as it is itself an invasion of privacy, but most of the time it is the *only* option available for making the surveilling heads accountable for their unscrupulous espionage. The ethicality of this act in the contemporary times is open to debate, as it has risen in response to the unjust commercialization of the internet, mass surveillance and surveillance capitalism, which are facilitated by our dependency on the internet.

Furthermore, my research reveals that the difference in the characterization of Ms Mistleto and Andreas Wolf parallels the difference of opinion between Jonathan Franzen and Eugene Lim regarding technology and resistance. Franzen, who is known for being suspicious of the technological and digital world, portrays Andreas Wolf as a rebelling subject obsessed with personal gain more than the welfare of the public. On the other hand, Lim, as one of the debut authors of this technological world, depicts Ms Mistleto, who, as a rebel, having noble intentions behind the enactment of the illegal acts, fights for the betterment of the masses. In spite of this difference in characterization, both novels indirectly justify cyberterrorism as an ethical act that is adapted to contest the corrupt powerful structures, as both of

the hacktivists bring justice in some form within the social structure.

Conclusion

The unjust workings of neoliberal capitalism and its manifestations have promoted the enactment of illegal acts such as cyberterrorism as the last option of resistance. This helped the rebelling subjects in enacting their agency with the hope to bring any positive change. My findings in this research have strengthened my claim and enabled a recasting of cyberterrorism as an act of ethical resistance. However, there are still multiple unexplored aspects that one can investigate when it comes to studying the phenomena of surveillance, cyberterrorism and ethical resistance. Research in these directions is the need of the hour since technology is dominating every aspect of our lives, and there is only a little research available on the topic of cyberterrorism and its ethicality as well as on the negative consequences of legalised surveillance.

Firstly, there is a need to contemplate over the topic of governmental surveillance and its poisonous repercussions in South Asia. It is evident that to study the ethicality of cyberterrorism, my research questioned the phenomenon of mass surveillance in general and in relation to the South Asian context. However, there is a further need to conduct more research on the consequences of surveillance capitalism in specific parts of the world, especially in different countries of South Asia. This could provide us with many new avenues of the complications of legalised surveillance through technological devices. These surveilling technologies manage civil populations and are mostly perpetuated to control the masses, especially the displaced and marginalised. Such research can therefore prompt further investigation of technology and mass surveillance, which I suggest, is a contemporary form of colonization when studied in specific contexts.

Secondly, it is apparent that my work has mainly focused on contextualizing cyberterrorism as an illegal but ethical resistance, and through this discussion it has debunked the myth of cyberterrorism as a threat. However, there is still a need to explore other modes of resistance that have been considered illegal but are technically ethical due to their contestation of unjust and exploitative governmental manipulations. Hence, we need to conduct research, specifically within literary studies, which challenges such unjust criminalization of rebels and highlights the lack of accountability on the government's part and on the part of other corporate structures along with their exploitation of the masses for financial gains. Since fiction is an imitation of real life and fiction has markedly influenced the human consciousness. While my research is a small step in this direction, further investigation of such topics can lead to opening a great number of avenues for more research in the field of literature.

References

- Anonymous. "Internet Privacy Laws Revealed - How Your Personal Information is Protected Online". *Thomson Reuters*. <https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online>
- Anonymous. "Pamela Anderson calls on Trump to pardon *WikiLeaks* founder Julian Assange". *Dailymail*. 7 Dec. 2020. www.dailymail.co.uk/news/article-9027821/Pamela-Anderson-called-President-Trump-pardon-Wikileaks-fugitive-Julian-Assange.html. Accessed 19 January 2021.
- Anselin, Luc & Sarah Williams. "Digital Neighborhoods". *Journal of Urbanism: International Research on Placemaking and Urban Sustainability* 9(4). 2016. 305-328.
- Assange, Julian, Jacob Appelbaum, Andy Müller-Maguhn, and Jérémie Zimmermann. *Cyberpunks: Freedom and Future of the Internet*. New York; London: OR Books Publication, 2016.
- Assange, Julian. *When Google Met WikiLeaks*. New York; London: OR Books Publication, 2014.
- Burch, Sally. "Exposing Abuse of Power: For the People". In *Defense of Julian Assange*, edited by Ali,

- Tariq & Margaret Ratner Kunstler, New York; London: OR Books, 2019. 226-235.
- Cadwalladr, Carole. "The Great Hack". *The Guardian*. UK, 20 June 2019. www.theguardian.com/uk-news/2019/jul/20/the-great-hack-cambridge-analytica-scandal-Facebook-netflix. Accessed 15 January 2021.
- Chiesa, Raoul, Stefania Ducci, and Silvio Ciappi. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (1st. ed.). Auerbach Publications, USA. 2008.
- Couldry, Nick. "The Price of Connection: 'Surveillance Capitalism'". *The Conversation*. 23 Sept. 2016. www.theconversation.com/the-price-of-connection-surveillance-capitalism-64124. Accessed 10 January 2021.
- Cumming, C. P. "Hacktivism: Will it Pose a Threat to Southeast Asia and, If So, What Are the Implications for Australia?" *Indo-Pacific Strategic Digest*, 2017. 269-280
- Curran, Kevin et al. "Cyber Terrorist Attacks". *Cyber warfare and cyberterrorism*. New York: Information Science Reference Publications, 2008. 1-6
- Denning, Dorothy E. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives. "Cyberterrorism" Global Dialogue, Washington, Washington D.C., May 2000.
- Dickens, Charles, and Charlotte Mitchell. *Great Expectations*. London: Penguin Books, 2003. Print.
- Dreyfus, Suelette & Julian Assange. *Underground: Tales of Hacking, Madness, and Obsession on the Electronic*. Reed Books Australia, 1997
- Gellman, Barton. *Dark Mirror: Edward Snowden and the American Surveillance State*. New York: Penguin Press. 2020.
- Hardy, Keiran, and George Williams. "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism". *Cyberterrorism: Understanding, Assessment, and Response*. New York: Springer, 2014. 1-23.
- Kamran, Hija. "Privacy-in-Law: How safe is your data?" *Digital Rights Monitor*. March 25 Issue, Pakistan' Digital Rights Monitor, 2021. Privacy-in-Law: How safe is your data? – Digital Rights Monitor.
- Kerry, F. Cameron. "Why Protecting Privacy is a Losing Game Today—and How to Change the Game" *Brookings*. July 12 Issue, 2018. <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>
- Mehan, Julie E. *Cyberwar, Cyberterror, Cybercrime: a Guide to the Role of Standards in an Environment of Change and Danger*. UK: IT Governance Publishing, 2009.
- Mikhaylova, Galina. "The 'Anonymous' Movement: Hacktivism as an Emergency Form of Political Participation" MS Thesis, Texas State University, 2014.
- Milone, Mark G. "Hacktivism: Securing the National Infrastructure." *Knowledge, Technology, & Policy*, 16(1) EBSCO Publishing, 2003, 75-103.
- Noble, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press, 2018.
- Radack, Jesselyn. "Assange and Whistleblowers". In *Defense of Julian Assange*, edited by Ali, Tariq & Margaret Ratner Kunstler, New York; London: OR Books, 2019. 324-326.
- Shapiro, J. Robert. "What Your Data is Really Worth to Facebook" *Washington Monthly*. July/August Issue, 2019. <https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-Facebook/>
- Snowden, Edward. *Permanent Record*. New York: Metropolitan Books/Henry Holt and Company, 2019.
- Verton, Dan. *Black Ice: The Invisible Threat of Cyber-Terror*. 2003.

Weimann, Gabriel. "Cyberterrorism: How Real Is the Threat?" Special Report for United States Institute of Peace. 2004.

Yar, Majid. *Cybercrime and Society*. Second Edition. London: Sage Publications, 2013.