Lapis Lazuli

An International Literary Journal

ISSN 2249-4529

www.pintersociety.com

GENERAL SECTION VOL: 9, No.: 1, SPRING 2019

UGC APPROVED (Sr. No.41623)

BLIND PEER REVIEWED

About Us: http://pintersociety.com/about/

Editorial Board: http://pintersociety.com/editorial-board/

Submission Guidelines: http://pintersociety.com/submission-guidelines/

Call for Papers: http://pintersociety.com/call-for-papers/

The Evolution and Features of Cybercrime Fiction

Himanshi Saini

Abstract:

The essay aims to look at the development of cybercrime in today's age of digitisation and how it has impacted the nature of crime. As a relatively new addition to the genre of crime fiction, cybercrime fiction addresses major issues about the changing nature of methodology of crime detection, and how that further develops the roles of the criminal as well as the detective. This essay aims to bring the fore the budding concerns of this new genre and how these concerns pave way for a nuanced understanding of the blurring distinctions in today's age between one's actual and virtual presence.

Keywords:

Cybercrime Fiction, Crime Fiction in Digital Age, Social Engineering in Fiction, Crime and Cybercrime, Nature of Cybercrime, Culture and Cybercrime, Cyberpunk and Cybercrime Fiction.

***

The nature of crime is ever evolving. It adapts to the changing social relations and incorporates technological advancements. The purpose of this essay is to trace the evolution of crime within crime fiction and how it catapults a new genre "cybercrime fiction" which primarily focuses on the incorporation of technology for the purposes of criminal activities. How this genre changes the role of the crime solver, the criminal and ultimately the very nature of crime? And how cybercrime fiction as we know it today came to be? These are the primary questions that this essay will seek to address.

The aim of this essay is to first trace the evolution of crime fiction and the various subgenres that have come to be a part of it and eventually look at the features of cybercrime fiction and figure out where this subgenre fits within the rubric of crime fiction. To further elaborate on the advances made in crime fiction I will be working with Ian Sutherland's *Brody Taylor series*, and Patrick Oster's *The Hacker Chronicles*. All these works are centred around the lives of white hat hackers who because of their meddling nature end up being part of criminal investigations and as such become propellers in solving the case.

Aware of the porosity and flexibility of the genre of Crime Fiction, critic John Scaggs models his analysis of the development of Crime Fiction on what he believes can be termed as Ferdinand de Saussure's diachronic approach. By tracing the genre's thematic and formal development vis-à-vis history he aims to essentially present his readers with the chameleon-like nature of the genre and how it skilfully adapts itself based on the socio- economic developments within the spatial as well as temporal spaces of the novels and those which the writers inhabit.

Tracing the crime back to the dramatic tragedy of Sophocles' Oedipus Trilogy, Scaggs tries to trace the moment when the act of murder finally becomes the main driver of the plot. It is with Edgar Allen Poe's *The Murder in Rue Morgue* that we finally begin to see the foundations of crime fiction being set in stone. What is truly remarkable about the genre of crime fiction is its extreme self-reflexivity which helps its enthusiasts truly trace its developments. The genre has been wrenched from the hands of elitists and given the space within the field of literary endeavours as a trend that is worthy of being studied to understand the change in the perception of the masses about how they understand crime and how this understanding of crime itself is also influenced vis-à-vis the depiction of murderers, detectives, conditions of the crime within the plot.

While tracing the development of Golden Age Detective Fiction to its hard-boiled counterpart in America founded by the likes of Raymond Chandler and Dashiell Hammet, we get to see the influence of the Depression Era in the creation of hardboiled fiction. According to critic John Scaggs, "Hard-boiled fiction translated the romanticism of the Western into a modern urban setting, and this movement from the Western frontier to a hostile urban environment was accompanied by an abrupt shift from the artificial gentility of the classical detective story to the creation of a fictional world of social corruption and 'real' crime." (34)

By taking the example of the creation of the subgenre of Hard-boiled detective fiction, I am trying to bring the reader's attention to the fact that the development of various subgenres of Crime Fiction are a result of changing historical, political settings which try to keep up with the changing nature of crime as well as its detection and then create fiction as inspired from these changing events. Looking at hardboiled detective fiction which developed in America in the late 1920s and 30s also helps us understand the roots of development of Cyberpunk fiction.

While tracing the development of this subgenre, it can be clearly seen that it develops as an offshoot of Cyberpunk fiction which has its foundation within science fiction. Although, much work has been done in defining Cyberpunk fiction, little to no work is available that actually discusses Cybercrime fiction.

Cyberpunk enthusiast David Cavallaro in his book *Cyberpunk and Cyberculture: Science Fiction and the Work of William Gibson* asserts that, "Dashiell Hammett's Red Harvest (1929) is a classic of hardboiled detective fiction that anticipates important aspects of cyberpunk. Its hero is a loner (like Gibson's Case, Turner and Laney, for example) who has to face up to an amorphous world of corruption and violence and juggle with this toughness as both a physical attribute and an intellectual faculty. The figure of the tough guy responsible for solving puzzles in a surreal setting of urban brutality deprived of any real sense of belonging and forced to do the sorting out singlehandedly, consolidated by another hard-boiled classic: Raymond Chandler's *The Big Sleep* (1939). "(10) He also further mentions several other points of influence for cyberpunk fiction which include dystopian fiction with its futuristic settings and dense postmodernist themes.

It is also worthy to note that the development of cyberpunk is not specifically limited to literary influences. It finds its core philosophy with advancements made in the field of cybernetics. The core philosophy driving the field of cybernetics according to mathematician Norbert Wiener in his ground-breaking work *Cybernetics, or Control and Communication in the Animal and the Machine*,

is that if the human body were to be seen as a machine and its functioning simulated via mechanical development and computer programming then it is possible to create a cybernetic organism. The most popular example out of popular media being the Arnold Schwarzenegger playing the role of the Terminator, in the movie Terminator 2: Judgement Day.

According to critic David S. Wall, Cyberpunk fiction had a huge impact of mainstream popular culture which in turn created a paranoia within the urban populace about the repercussions of uncontrolled technological innovations. In his essay "Cybercrime and Culture of Fear", he points out that

> "Drilling down for an explanation of the contradictions between what people say and what is happening (such as prosecutions) reveals the presence of a mythology, or a series of myths about cyberspace and cybercrime. This mythology arises from a combination of distortions in the ways that knowledge about cybercrime is produced and cybercrime's powerful cultural antecedents in social science fiction… The mythology emerges when fictional ideas subsequently that frame concepts and become presented as truths that reinforce public anxieties and apprehensions." (861)

In these lines David S. Wall is primarily dealing with the impact that Cyberpunk fiction has had on the public perception of cybercrime. He further discusses how this perception has actually fed into the creation of governmental policies on internet crime and the need to protect the public interests. He points to the problem within this situation because according to David S. Wall the public paranoia of technological future is far from turning into a reality. In his other works he also discusses how there is little that has been done in terms of statistics of cybercrime and rather than create a global network of criminals' intent on disturbing world peace, the internet had facilitated has actually paved the ground for better global communication. And very little is ever present in cyberpunk fiction to prove that.

While this is clearly the case of cyberpunk fiction which more often than not looks at the ultimate end of technological revolutions, with notions of concepts like virtual reality being taken to their extreme (the Wachowski Brothers' Matrix being an example), the same cannot be extrapolated for cybercrime fiction. Although cybercrime fiction has come to the fore after cyberpunk, its concerns are not futuristic. It looks at technology as it is used in contemporary society. The purpose of the writer is to expose the kinds of crimes that are possible via cybercrime with today's technology. There is little in cybercrime fiction to do with theoretical speculations.

However, that does not mean that cybercrime fiction doesn't ultimately create a kind of mass paranoia of its own. With hacker detectives as the main protagonists of the plot, who more often than not are cybersleuths the idea of illegal surveillance and lack of privacy is one of the prime plot drivers of this kind of fiction. (The case of Ian Sutherland's *Invasion of Privacy* and Patrick Oster's *The Hacker Chronicles*).

Critic Sheila Brown in her essay, "Fiction, Fantasy and Transformation in the Imaginaries of Cybercrime: The Novel and After" notes that, "It is certainly the case that fictional representations of the cyber and its crimes after the mid-1990s

began to depart decisively from their association with street or counterculture, and certainly were no longer dominated by futuristic science fiction as such." (156). Cybercrime fiction takes up the realist mode and is "driven more by DNA codes, forensic analysis, computer databases, electronic surveillance and dataveillance, pattern analysis, voice and face recognition software… and so on. What cyberpunk extrapolated into a different dimension of being, detective fiction embraced in painstaking detail to make itself more real. (159)

Taking Ian Sutherland's Brody Taylor series as an example we get to see, that there is remarkable similarity in the creation of the hacker-detective figure as there was in the case of the amateur detective. The hacker is often a lone figure who occupies the moral grey area within the scope of the fiction as he uses illegal means to get the job done. He possesses the knowledge that the official institutions lack and is willing to overstep bureaucratic hurdles in order to get to the criminal. He is a privileged individual, who consciously chooses to call himself a white hat hacker, in that he only hacks for noble reasons and not for the invasion of privacy. Brody Taylor in Ian Sutherland's fiction is a white hat hacker, who helps international conglomerates improve their security. He is contracted by these companies to perform penetration tests on their technical setups to help expose their vulnerabilities so that they can work out the kinks and keep their data safe.

The first part in the series titled *The Social Engineer* also introduces the readers to an interested trope that is often used within cybercrime fiction called social engineering, which can actually be considered a fancy term for moving in disguise, where Brody Taylor uses several disguises both online and offline to dupe people into revealing sensitive information which can then be used to hack the servers of the company by potential white hat hackers.

It is Brody Taylor's ability to overlook moral qualms about certain hacking activities that actually make him indispensable for the police forces. The novel *Invasion of Privacy*, shows him participating in an illegal penetration test to prove his hacking superiority vis-à-vis his internet handle Fingal. He is challenged to penetrate a website called 'secretlywatchingyou.com', which is an illegal surveillance website that has become a hub for internet voyeurs as it has hacked into the video feeds of many homes and is displaying intimate moments of their lives, a real live 'Big Brother' is you will. While trying to penetrate the security defences of the website, Brody happens upon a criminal investigation and gets involved in helping to get the criminal. This is how the initiation of Brody Taylor within the work of crime is brought about.

The most basic definition of cybercrime is usually crime which is committed with the help of the computer. However, the matter of cybercrime is far more complex than that. Cybercrime fiction features criminal activities which could not have taken place without the use of the internet, or criminal activities which can be tracked via the use of technology.

The figure of the hacker is a computer genius, willing to work with authorities to bring criminals to justice. Their skills of detection are not from visiting the crime scene, but from working behind the computer screen. In today's urban existence there is little that has not been touched by technology. With our presence on social media and every individual owning a smartphone, it's not too difficult to track one's whereabouts and daily habits. The hacker figures often

used these dependencies of the victims to their advantage to help track criminals. They are not characters who have any murder detection skills per say, which is why they work in collaboration with the police forces who have those skills and help them track criminals that they don't have the technical expertise to track. It is more to do with tracking the virtual footprints of the criminal as opposed to tracking the actual footprints.

In such fiction the criminal may or may not be a hacker. However, it is usually the case that the protagonist of the work usually is one. The perpetrator of the crime may or may not be technically skilled. In the case of Ian Sutherland's *Invasion of Privacy*, where the plot focusses on a website called 'www.secretlywatchingyou.com', two perpetrators are apprehended. The first one is the creator of the website, who via his website has given access to internet voyeurs to pry on private lives of people without their knowledge. The second perpetrator is a customer of the website who has been using the website to track his potential victims, spy on them and finally plan his murders by luring them to locations. The second perpetrator is not a person who is technically skilled but the website has given him the opportunity to successfully plan his kills in ways that have kept him undetected for so long.

As such cybercrime fiction deals with certain very important ethical issues of creation. The internet makes it possible to make new applications whose intent is less ethically driven and more profit driven. As the investment in creation of illegal websites and web applications is not on a massive scale, the internet provides a whole global market for access, the advantage of making exponential profits is always there which is the prime reason why in the recent decades the internet had become a growing hub for criminal activities.

Cybercrime fiction deals with the moral ramifications of access to such global networks, where criminals can function with anonymity. Anonymity in cyberspace comes with its own benefits and drawbacks. While it gives voice to the weak, for example helping abuse victims find forums where they can discuss their personal traumas without the risk of any shame, but it also creates the space for cyberbullies, who might just use such forums to initiate debates which are racist, sexist or fundamentalists.

At what point can authorities step in and monitor such discussions and reduce negative influence is where the matter gets extremely complicated. Although , filled with suspense, the prime driver of the plot is rarely to simply figure out who the perpetrator is but is the thrill that the readers would get in watching the hacker display his skills to hack into mainframes and extract sensitive information that usually helps in solving the case. This type of fiction is littered with technical references and it is the skill of a good writer to help their readers understand them. It often creates a sense of triumph for the readers to understand how exactly a hack is done.

Just like any other genre of popular fiction, cybercrime fiction is not far away from creating its own stereotypes in terms of creating the image of black hat hackers. As the works mentioned in this paper are written by British or American authors, when presenting the internet mafias, particularly drug trafficking or sex trafficking rings the focus usually goes towards Russian hackers or terrorists from the Middle East.

The narrator of *The Hacker Chronicles* when discussing black hat hackers elaborates, "You cyber-newbies need to know that the white hats get paid a ton to track down black hats – the Russians, the Chinese, the mob guys, crazy independents and, these days, the North Koreans or the Iranians." (Oster, ch.3.) As such, just like Golden Age Detective fiction there is lot more to say about the presentation of crime within cybercrime fiction that meets the surface. There is clearly an element of myth making in terms of the ideas of criminal figures belonging to certain nationalities. These are rising points of contestations that need to be addressed in academic discussions.

Surveillance and lack of privacy are other tropes that this type of fiction loves to exploit. It more often than not functions as a warning bell for the dos and don'ts for the tech savvy age. While it does presents the readers the dangers of internet surveillance, it also presents them with solutions to protect themselves from being hacked, or by not posting details about their lives that might be misused if given in the wrong hands.

Unlike its parent genre, which seeks to show technology's ugly mask, cybercrime fiction tries to strike a balance for the readers to see how there are certain simple ways via which a person can actually reduce the risks of becoming victims to black hat hacking attacks.

The methods via which the hacker figures are able to track the criminals usually show that there are two sides to the coin. As crime has evolved to incorporate the internet for its smooth functioning so has the detection of crime as well. Cyberspace is still an open terrain and crime fiction becomes a good place for readers to become aware and spark up a debate about the use as well as abuse of information in today's date. Its stylistic realism is able to create a ground the issues of cyberspace are no longer within the hypothetical domain. Illegal surveillance, abuse or private data are very real threats within the legal and criminological discourse. There is a definite need to reimagine crime and reformulate ethical boundaries that help citizens of the world keep their freedom and not give them the liberty to abuse it.

These works also tread a thin line in terms of raising questions about policy making, which is a relatively new terrain for internet surveillance policies. To what extent can control be sanctioned to the state? How much privacy is the state at liberty to gain access to? The problems of dealing with global crime rings and how to deal with countries which have lax hacking policies that make them a prime spot for the setup of crime bases. These are questions that are brought forth by Cybercrime fiction.

Although, not many works have been published that specifically deal with this subgenre, however the potential is still there. The slow rate of growth for this subgenre, could be the need for a certain level of programming and technical skills as well as the rhetorical skill to create a challenging yet gripping page turner that would appear to the readers of such popular fiction.

Cybercrime fiction seeks to address the fact that the threat of internet crime in cybercrime fiction is very real. And the difficulty of the governance of surveillance. And it presents the readers with ideas of the evolution of means of prevention of crime, an issue that cyberpunk fiction rarely addresses. It has the advantage of a very rich tradition behind it. As such formulaic creation of

this type of fiction is just as playful as Golden Age fiction once was. However, when I say formulaic I don't mean any rigid cocktail recipe that cannot be experimented with. As the subgenre is new and still developing, there are many areas that are open to exploration.

In a global and capital-based economy the definition of crime is ever evolving, to pin it down to a rigid definition would be to underestimate its potential, this is where the contributions of crime fiction become contributing. The power of narrative helps the readers skip through the jargon of legal and criminal discourse and effectively delve understand issues and problems of social media on which the people are increasingly becoming dependant.

Another important issue that is frequently being addressed in cybercrime fiction and media as well is the idea of the cryptocurrency and how it has become a prime facilitator in drug and sex trafficking activities. The success of Bitcoin and the current battles in different nations over the legal efficacy of such currency are important issues that need to be discussed and raised at a socio-political level.

As a consequence, what we get to see is that this kind of fiction doesn't change the nature of crime but shows the how technology has accelerated the process of crime, with increased surveillance and ease of access to information. How according to David. S Wall this 'culture of fear' within the people has produced a paranoia among people who are increasingly resorting to counter-surveillance methods, for example parents demanding electronic surveillance within classrooms to govern the safety of their children.

These are debates that have increasingly gained interest in today's age. The closing section of this article merely addresses the instability of the cyberspace and the constant need to counteract its negative effects which has led to worldwide concerns. The questions left for the readers are; can Cybercrime fiction truly pick-up where cyberpunk left off? Would it be able address the issues of virtual identities and their 'white hat and black hat' potentials? Will this subgenre gain the popularity of its antecedents?

WORKS CITED:

Brown, Sheila. "Fiction, Fantasy and Transformation in the Imaginaries of Cybercrime: The Novel and After". *Handbook of Internet Crime*, edited by Yvonne Jewkes and Majid Yar, Willan Publishing, 2010, pp. 145-166.

Cavallaro, David. *Cyberpunk and Cyberculture: Science Fiction and the Work of William.* The Athlone Press, 2011.

Oster, Patrick. *The Hacker Chronicles.* Padraig Press, 2017.

Poe, Edar Allen. The Murders in the Rue Morgue and Other Stories, Willside Press, 2011.

Scaggs, John. *Crime Fiction: The New Critical Idiom.* Routledge, 2005.

Sophocles, Oedipus Trilogy. Translated by Patrick Mullahy, Read Books, 2011.

Sutherland, Ian. *Social Engineer.* Brookman Books, 2014. Ebook.

---. *Invasion of Privacy.* Brookman Books, 2014. Ebook.

---. *Taking Up Serpents.* Brookman Books, 2014. Ebook.

Wall, David S. "Cybercrime and Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime", Information, Communication & Society, vol. 11, no. 6, 2008, pp. 861-884. papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155

Wiener, Norbert. *Cybernetics, or Control and Communication in the Animal and the Machine.* Martino Fine Books, 2013.

BIO-NOTE

Himanshi Saini works as an Assistant Professor (Ad Hoc) at Lady Shri Ram College. She has done her BA and MA in English from Delhi University. She is currently pursuing M.Phil in English from Delhi University and is in the midst of researching for her dissertation. Her topics of interest are Genre Theory, Popular Fiction, Narrative and Literary Gerontology in Indian Literature. Her teaching areas are Postcolonial Literature, Modern British and Postmodern British fiction and poetry, World Literature and Literary Theory.

E-mail: himanshi1491@gmail.com