Abstract

Though created few decades ago, cyberspace is deeply penetrating into our social and ethical mainstream. Reducing life to a non-physical environment, cyberspace serves as a proper application of some distinct posthuman ideals. A disembodied realm which supposedly liberates us from biological constraints, challenges strict forms of dualism and radically alters our sense of boundaries, cyberspace provides us with a rare opportunity to experience a posthuman future where we deliberately abandon our bodies. Still desirable though with its many defaults, cyberspace proves to be a barrier to regulations. It exposes inherent limits and effectiveness of our contemporary legal systems especially in fighting digital crimes. Filtering our human features not only our photos or videos, cyberspace represents a primitive posthuman scenario in which technological innovation would bring about the end of humanity as Posthumanism predicts. A posthuman novelist, Dan Brown, in his Digital Fortress (1998), suggests more realistic scenarios for human extinction. He exposes a posthuman concern regarding digital crimes and agitates contemporary sensitive debates revolving around fake identities.

Keywords: Cyberspace, posthumanism, invasion of privacy, digital crimes, cyber-attacks, Dan Brown, Digital Fortress.

المستخلص

بالرغم من أن الفضاء السيبراني قد تم انشائه منذ عقود قليلة إلا أنه يعد من أهم الجوانب الأكثر تأثيرا على الحياة الاجتماعية وكذلك الأخلاقية. وبعد الفضاء السيبراني من أهم التطورات التي لم يكن الوحيد الذي يمثل أهم مبادئ وأفكار الفلسفة المرة الإنسانية. حيث نحاول الفضاء السيبراني يخطط جميع العقبات البيولوجية والثقافية والقضاء على الانزواء الفكرية لتبدأ الإنسان المعاصر بفرصة نادرة لتجربة العيش في بيئة ماراوية خام بذلك ما فيها من مميزات وعيوب. وعلى الرغم من جاذبية الفضاء السيبراني والمداومة على استخدامه بصورة شبه يومية من قبل الكثير من المستخدمين إلا أنه أثبت بصورة قطعية في بعض النظم القانونية في محاسبة الكثير من الجرائم وخصوصا الجرائم الإلكترونية. ومن ثم فإن الفضاء السيبراني يمثل أحد أهم التهديدات التي تشارك بشكل فعال في الفضاء على الإنسانية المعاصرة كما انتشرت الفلسفة المرة الإنسانية. يقترح دان براون (ككاتب روائي) بنتمي إلى ما بعد الإنسان (1988) في روايته الحصن الرقمي (1998) سيناريوهات أكثر واقعية لانقراض الإنسان. يكشف محاوحا ما بعد الإنسان فيما يتعلق بالجرائم الرقمية ويتبرر مجموعة من القضايا المعاصرة التي تدور حول الهويات الزائفة.

الكلمات المفتاحية: الفضاء السيبراني، مرأة الإنسان، التهاون الخصوصية، الجرائم، الهجمات الإلكترونية، دان براون، الحصن الرقمي.
Cyberspace in Dan Brown's *Digital Fortress*: A Posthuman Study

by

Dr Ayman Ibrahim Elhalafawy
An Associate Professor of English Literature,
Faculty of Arts, Kafrelsheikh University

Becoming one of the defining features—if not the only one, of our contemporary culture, cyberspace is exceptionally a fast conquering disease. Though created few decades ago, our social life is evidently tangled and simultaneously unbearable without cyberspace. A perfect example of a post-anthropocentric posthuman domain where we deliberately abandon our bodies, since the beginning of the new millennium, cyberspace has become an integral part of our daily routine.

Almost half of the world population has direct access to different social platforms like Facebook, Twitter, Instagram, TikTok, etc. In an era of connectivity, a vast portion of population is texting, sharing hobbies, engaging in public discussions and transforming money freely. A different portion is using cyberspace to develop a business—paying or selling practically anything, without a third party asking for commission, or to hold meetings via different programs like Meet or Zoom which proved to be exceptionally useful during the quarantine.

Undoubtedly, cyberspace has proven its power during the curfew that was imposed on the entire world due to the outbreak of corona virus. During the quarantine, cyberspace did not only participate in raising people’s awareness but was the only available medium for communication. It became the place where people get rid of their depression by watching favorite videos or movies or by downloading favorite games or apps. Seen to increase intimacy among different generations, cyberspace became a place where long-distance relations can flourish. It became a place where introverted individuals could gain the capacity to form emotional ties and to be more socially interactive even without revealing their true identity.

Forming a union with ‘handheld devices’ which were becoming more popular among young generations, cyberspace became a propaganda tool not only for corporations but for political parties trying to put an end to traditional campaigns and gain wide acceptability among youth. Not restricted to individuals, different infrastructures and government sectors systematically became dependent on cyberspace. In a more coherent manner, most government agencies turned to digital transitions to ease congestion. In this context, cyberspace obviously
proves how "information technologies will continue to be imbricated with everyday life" (Lyon 32) and speed would be the only variable parameter that would really matter.

Nevertheless, it is not practically beyond our grasp that with enormous benefits come inevitable threats. Spending from nine to twelve hours daily on violent and sometimes destructive games like Pubg or El Hout El Azraq (Blue Whale), those games became the newest and most serious form of addiction. It is also estimated that average users spend from four to five hours a day surfing the internet; wasting almost one third of their lives on cyberspace.

Various studies have shown how filters used in some popular ego-smashing apps including Snapchat or Instagram would affect the mental health and in severe cases lead to depression and suicide. In another dimension, almost every woman who publishes her photo via different platforms suffers from cyber-harassment and cyber-stalking. Though the civil rights act of 1964 and the federal cyber-stalking law of 1968 systematically classified digital-harassment and digital-stalking as crimes, in most cases-afraid of their nude photos published without permission, most victims were forced to go-offline or shut down their profiles.

Another app known as TikTok which is quite popular especially among young generations is penetrating into our social and ethical mainstream. With dancing trends and ridiculous challenges which go viral and reach millions of hits in hours, it became exponentially hard to practice censorship or enforce a ban on inappropriate conducts that most underage users watch without supervision. Most of those users either choose to live on screens of their mobiles or follow thousands of bloggers or influencers.

Posting a signature on our social mainstream, cyberspace is not only seen to participate in the loss of an integral part of humanity by turning sentiment into emojis but to create a hybrid dialect within which technical verbs like scan or delete became part of our daily expressions. Turning hackers into digital heroes, this unprecedented flow of information demonstrates the power of technology which constructs humanity and shapes public awareness. Though television was criticized for the same reasons, with television "the motives are so clear. But what happens when the motive is not so obvious?" (Lessig 220). Apparently, "if speed is the essence of war, and technology is the enemy, then we are dead" (Dixon 166).
Also penetrating into our ethical mainstream, cyberspace is increasingly becoming a hostile environment that could be used for malicious purposes. A golden age for espionage, most agencies won’t bother sending field-agents while everything is available online. At this juncture, the influence of cyberspace on terrorism can no longer be ignored. With every aspect in our contemporary life controlled by computers, it is not practically a fanciful nightmare to suspect that terrorists would launch unavoidable cyber-attack on some of the most ‘critical infrastructures’.

By a single press of a bottom, terrorists could halt or determinate life itself and create a cyber-ice age. Crucially, with this software or digital currency which was invented in 2008 known as the bitcoin with no central authority nor taxes or even a paper trail, it has never been easier for terror organizations to work and to perfectly cover their tracks. Yet, most governments are spending billions of dollars to enhance such systems to be more resilient against cyber-attacks.

This enhancement came at the very expense of our digital privacy. Electronic terrorism became an excuse for developing a culture of secrecy and a guardian totalitarian state. Failing to neutralize cyber-threats, most governments take cyber-terrorism as an excuse for snooping and monitoring private emails. It became an excuse for monitoring login activities, personal records and "in some cases our every keystroke, is recorded"(Reed 60). Every move we make on/out cyberspace is recorded with high-tech surveillance techniques. This surveillance mania reached an alarming rate with a camera for every citizen in both America and China.

Without engaging in a heated dispute of whether violation of privacy does or does not undermine human dignity, invasion of privacy is not often restricted to government agencies. Practically, every corporation from Facebook to WhatsApp or Instagram retains a copy of our personal data, online activity and preferences that would be used in ‘unwarranted publicity’. Even with data protection policies, online regulations or global agreements, cyberspace does not seem to be a safe or a free realm anymore but a place for remote exploitation and organized crime. This very remark provokes a rather important question: should or should we not retreat to a more circumscribed life-style known before cyberspace?

Still desirable though with its many defaults, cyberspace proves to be a barrier to regulations. It exposes inherent limits and effectiveness of our contemporary legal systems especially in fighting digital crimes. Filtering our human features not only our photos or videos, cyberspace represents a primitive posthuman scenario in which technological innovation would bring about the end of humanity as posthumanism predicts.
Trying to avoid some of the most vital mistakes of practically all post-war movements, posthumanism which came to be recognized as an accurate depiction of our contemporary era attempts to properly extract humanity and challenge strict forms of dualism. By breaking ties with deep-seated assumptions and denouncing inherent superstition, posthumanism attempts to transcend disconnection which isolated humanity for decades. Though it was hard to reconcile a precise definition of the term, in *Philosophical Posthumanism*, Ferrando indicates how posthumanism can be described "a post-humanism, a post-anthropocentrism and a post-dualism; these three aspects should be addressed in conjunction"(54).

Ideologically speaking, posthumanism flourished as a rejection of traditional perception of human centrality. It is taken by many to become an apparent phenomenon by the year 1946 to 1953 (Wolfe xii). It is, as Braidotti proposes in *The Posthuman* "the historical moment that marks the end of the opposition between humanism and anti-humanism"(37). It mainly provides a new conception of agency that seems to take hybridity to a whole new level. This hybridity directly corresponds to the demands of Animal Rights/Protection Movements which require a higher ‘level of altruism’.

Promoting mechanical values, posthumanism provides alternative way of perceiving personhood and attempts to reconfigure humanity’s place in the universe making it open to radical transformations. Originated with anti-humanism, posthumanism seeks "a cosmology that would assert the essential dignity of animals without losing sight of what is uniquely human"(Steiner 251). Simultaneously, it urges humanity to respond to the world of both animals and synthetic intelligence. It attempts to help humans overcome ‘systematic discrimination’ and hitherto avoid extinction.

While we viciously struggle to transform our appearance either through plastic surgery or inserting metal rings or earrings in our face, nose or even a belly, posthumanism affirms the need for far more ‘effective regulations’ and ‘preventive ethics’. With a robot replacing the Vitruvian man, posthumanism puts forward the claim that synthetic intelligence exposes better ‘ecological harmony’ and retrieves data from the environment away better than humans could ever anticipate.

Staring at the possible ruins of our posthuman future, posthumanism illustrates how speeding up our ‘evolutionary process’ we may cause far more drastic consequences. Claiming that machines could learn through experience, Moravec insists that "robots would be able to handle programs that had a great many alternative actions at each stage of
a task—such alternatives would give the robot a wide margin for creativity" (47). This creativity would enable autonomous machines to "adapt and learn: qualities that are so fundamental to human nature" (Pepperell 8). It precisely comes down to the very fact that from the way we deal with technological advancements, we are causing our own extinction not domestic cyborgs which would share the same womb with us in the near future.

Inviting humanity to take few steps back, posthumanism mainly attempts to evaluate in a balanced manner moral implications that would result from granting the same prerogatives to nonhuman entities. Submitting a warning to a dying humanity, posthumanism urges us "to read the 'post' prefix in term 'posthuman' as signaling something that comes after the human, but remains in a continuum of human existence" (Toffoletti 12). In so doing, we could recognize which modes of humanity need to be retained and others which must be discarded. By maintaining a positive account of technology, as posthumanism suggests, we could avoid the upcoming war which we may call the Fifth Generation War.

This war is expected to be between common users and corporations who would have complete access to channels and platforms that practically only five percent of world population knows they exist; between those who could afford genetic enhancement and those who could not. Turning ourselves to cyborgs—half humans and half machines, this war would be between those cyborgs and their ‘artificial progeny’. By assigning a social role as an authority in the beginning of an era of synthetics to this progeny which lacks a moral sense, the future would apparently be owned by a small handful of cyborgs who would obtain power, funds and knowledge.

Nevertheless, without deducing posthumanism to its mere transcendental faculties, we could attend to a belief in overlapping substances and a strict commitment to achieve justice among such substances without being interwoven in our own existence as Foucault argues. Paying proper attention to the growing negative portrayals of rabid technological advancements, we must make sure not to be caught in a hip-hob dance with no standards nor procedures.

While the aggregate ethical dilemmas are never in decline, by addressing one and not practically a new recurring theme, Dan Brown (1964— ) whom we could label—though with precaution, a posthuman novelist seems to perfectly tackle some of the most prominent aspects governing posthuman reasoning. Hoping to contain the problem even
before it erupts, *Digital Fortress* (1998)- written two years before the emergence of different social platforms, depicts cyberspace as a threat and highlights using cyber-terrorism as an excuse to violate digital rights. It mainly foreshadows essential ethical questions related to cyberspace morality and digital privacy.

A posthuman novelist, Dan Brown suggests more realistic scenarios for human extinction. He exposes a posthuman concern regarding digital crimes and agitates contemporary sensitive debates revolving around fake identities. Exposing the failure of our contemporary ethics to condemn those who commit crimes using fake identities, Brown suggests that our failure to develop a techno-ethical system in a techno-scientific environment would cause far more serious implications.

By drawing the attention of legal scholars to such threats, Brown seeks to expose a rather urgent need to update contemporary legal systems to reflect emerging realities and to provide a basis for intelligent behavior. He mainly intends to open up a discussion of socio-ethical dilemmas that unlike bioethics hardly gain proper attention among scholars. Hopefully, legal scholars and policy-makers could develop an ethical framework that can be functional in the real world as well as the virtual.

Born deformed, Ensei Tankado was a crippled genius with twisted fingers. Before he was born, Tankado’s mother traveled to Hiroshima to help in the burn centers. It was then when she became one of the radiated people. Given birth to Tankado at the age of 36 she bled internally and died. Losing his wife and ashamed of his deformed child, Tankado’s father abandoned him in the hospital. As a boy, Tankado swore to take revenge from the country that killed his mother and ashamed his father.

Placed in different foster homes, when he was twelve, Tankado was invited to take part in a test for a new keyboard developed for handicapped children. It was then when Tankado discovered his love for algorithms. At the age of twenty, Tankado earned a scholarship to Doshisha University. He became a figure among programmers and made fortune by writing algorithms. Developing devotion for Buddha, he soon forgot his vow of revenge. After his hatred faded, NSA courted him.

A top author of algorithms, Tankado was working on a massive project known as TRANSLTR. This TRANSLTR is a multibillion dollar computer which uses "the power of parallel processing as well as some highly classified advances in clear text assessment to guess pass-keys and break codes"(Brown 16). TRANSLTR for NSA was "a child of necessity"(14). A great success, TRANSLTR managed to locate sixty-four pass-key in less than ten minutes. Thus in order to avoid civil rights
rejoicing about violation of rights and ensure that terrorists would keep using their emails, NSA leaked information that the project was a complete failure.

A brilliant programmer, Tankado was "kind and honest, and of impeccable ethics. Moral integrity was of paramount importance to him. It was for this reason that his dismissal from the NSA and subsequent deportation"(24). Working for NSA, Tankado was convinced that the use of TRANSLTR would be regulated by the justice department. And for any e-mail to be deciphered it needs a ‘federal court order’ just like the one needed to install a wiretap which would prevent intercepting private emails.

However due to time pressures, as the staff was told, TRANSLTR "was to be a free-standing decryption device whose day-to-day operation would be regulated solely by the NSA"(24). This change in plans meant gross violation of privacy. For Tankado, it was like "having a bug in every phone in the world"(24). It meant that NSA would be able to decipher any email even of law-abiding citizens. Like Greg Hale who shares the same viewpoint and who was his only friend in NSA, Tankado believes that snooping citizens without a warrant is a serious violation of digital privacy.

Tankado believes that getting an information source like TRANSLTR is a tricky responsibility NSA is not just ready for. In this respect, Greg Hale asks some legitimate questions precisely: "what happen when some future government doesn’t have our best interests at heart! This technology is forever!"(182) and how would "civilians defend themselves against a police state when the guy at the top has access to all their lines of communication? How do they even plan a revolt?"(182). Thus, he attempted to violate NSA’s code of secrecy by contacting the press. He attempted to contact with one of civil rights movements known as Electronic Frontier Foundation (EFF)

Therefore, in order to avoid the mass hysteria or the intelligence nightmare that the news about TRANSLTR would cause, Tankado was captured and deported. The damage-control specialists in the NSA also destroyed his reputation and accused him of spying. Leaking this news, nobody would believe his story of a massive ‘code-breaking’ machine. Though he was assured that only emails related to crimes would be recorded, Tankado became outraged. He decided to make TRANSLTR obsolete and destroy the beast himself.

Fighting to death for the right for privacy, Tankado wrote an algorithm which creates unbreakable codes-namely, Digital Fortress. After writing his evolutionary algorithm, he posted an encrypted copy of
it at his internet site so that everyone could download it but cannot open it. Holding NSA hostage, Tankado threatened to give the pass-key that can open digital fortress to the highest bidder unless they reveal the truth about TRANSLTR to the world. Understanding that they would be helpless without TRANSLTR and that this algorithm would make cryptology a ‘dead science’, they targeted Tankado and killed him.

Seconds before his death Tankado gave away his ring on which he engraved the pass-key to a complete stranger as a farewell gift to the world. Soon after his death, they discovered that Tankado’s original target was never TRANSLTR which has nothing stored inside but NSA’s main databank; the backbone of U.S operations. Practically, his algorithm was nothing but "an encrypted virus, probably sealed with some generic, mass-market encryption algorithm, strong enough to keep everyone out of harm’s way—everyone except the NSA"(185). Crucially, TRANSLTR was the only device powerful enough to crack the seal and release the virus.

Tankado attacked NSA’s main databank with a worm which was simple with no ego or complex structure. It is programmed to do its work and check out or commit ‘digital suicide’. Worms of this sort are "stand-alone programs that replicate by spreading copies of themselves together systems through a network"(Chen & Davis 18). This picky worm could "delete files, or it might just decide to print smiley faces on certain white house transcripts"(226). Nevertheless, it was mainly targeting the same security filters which keep the databank save from prowling hackers trying to have a peek. This databank practically has got five levels of defense—mainly, a "primary Bastion Host, two sets of packet filters for FTP and x-eleven, a tunnel block, and finally a PEM-based authorization window"(299). Destroying those filters, classified data would become a ‘public domain’ available to everyone.

Fishing for fools, Tankado captured the biggest whale—Trevor Strathmore. After Tankado’s deportation, Strathmore—the deputy director of NSA’s operations, had to make sure that the truth about TRANSLTR remains hidden. With hard-nose efficiency, Strathmore was intercepting and reading Tankado’s emails. Reading one of Tankado’s emails, he knew about the ‘brute force-resisting’ algorithm which he developed. Known for his ‘cogent reductive’ analysis, Strathmore was not going to let digital fortress which he sees as a life-time opportunity to slip away. Blinded with ambition, Strathmore wanted to retire with pride; knowing that he made a difference. Hence every move he makes is always meticulously planned; Strathmore developed an intelligence scheme of facilitating the release of Tankado’s algorithm only after he rewrites it and inserts a backdoor.
Strathmore planned to insert a few lines of ‘cunning programming’ known as backdoors. With this smooth switch, NSA would hold the master key to every code written in the globe. Being able to see past moral perplexities, Strathmore insisted that "people have become paranoid. They suddenly see us as the enemy. People like me and you, people who truly have the nation’s best interests at heart, we find ourselves having to fight for our right to serve the country"(162). Believing in the righteousness of his own motives, he further insists that "there are naïve people in the world, people can’t imagine the horrors they’d face if we didn’t intervene. I truly believe it’s up to us to save them from their own ignorance"(162).

Being crippled by the bombs, Tankado’s ultimate revenge of NSA was in a form of a bizarre question which he left as a clue to guess the correct pass-key. Behind the scenes even after his death mocking NSA, Tankado challenged them to find out the prime difference between elements responsible for Hiroshima and Nagasaki. Knowing that they had different fuels plutonium and uranium, Susan and David soon figured out the correct pass-key. Practically all along, Tankado did not dumb his ring. He was trying to communicate, waving with his three deformed fingers to tell NSA whom he knew were watching the pass-key. Apparently, Tankado never intended to reach this far. He only wanted a confession from NSA of TRANSLTR; performing the simplest known form of digital extortion. Nevertheless, thinking that Digital Fortress written two years after its publication with the advancements of different social platforms including Facebook, Twitter or Instagram, we could surely expect totally different scenarios. Julian Assange and Snowden are practically perfect examples of which scenarios to be expected.

Publishing confidential documents in 2010, Assange suffered from political persecution. Spending over than a decade in confinement, his actions yet serve as a warning to governments thinking themselves immune to hacking and digital threats. Simultaneously, being able to stop Tankado’s worm only before destroying the last and final filter by just a fraction of a second, Brown hopes to contain the problem even before it erupts. Suggesting that there would literally be no secrets, Brown seamlessly imposes a rather important ethical question: is computer hacking even for ethical purposes ethical or not?.

Depicting cyberspace as a threat, Brown suggests that being anonymous cyberspace would become a domain in which we can/choose to dress up as someone else completely and behave differently. This difference "may have to do with the notion of being convinced of the reality of someone or something"(Ploug 8). Practically, anonymity could
bring out our worst features. Being free to defy ethical norms, it could fuel both ‘vices and virtues’. Thus, if isolation is a vice as developers of different platforms often claim then ethically conscious users must be always skeptical.

In using cyberspace we must perfectly choose what to believe and what to publish or share. Also, programmers or developers must understand that living by a code as a regulation is not sufficient anymore. Logically speaking, this social contract we live by is no longer suitable in an information age which does not yield the prospect of a just community. Living in age of transition, as Braidotti explains, "we are not always lucid or clear about where we are going, or even capable of explaining what exactly is happening to and around us. Some of these events strike us in awe and fear, while others startle us with delight" (196).

Thus what programmers must do is to provide the basis for intelligent behavior. They must manage this fear of electronic terrorism which radically alters the attitude and value of the victims and motivate certain social and ethical values that could cause a massive change in behavior on cyberspace. Those forgotten values should not remain intact as the theoretical basis for academic trends. As, those values could "speak to huge global problems rather than serve as a passive ideology that functions only for philosophers" (Hernandez 117). Practically, if such values are either "destroyed through overtly evil cruelty or quietly eradicated through a commitment to a mechanistic view of human significance, the flood gates of human rights violations will be opened" (111).

Hitherto, understanding the limits of our contemporary laws, seeking ‘civil remedies’ would be one of the possible solutions that would help us bridge this gap between humans and posthumans without losing our humanity. Seeking refuge in our social environment, we could restore those values and promote ‘ethics of care’ which could combat ‘destructive attitudes’ on cyberspace and abolish a wide range of social threats including cyber-stalking, cyber harassment, exploitations and sexual abuse without turning a blind eye on violation of basic human rights.

Hence change has never been swift, we must understand that a future with untapped possibilities even if such possibilities are opened by our social position as historical entities is better than no future. The point here is that updating traditional human values and extending human morality may be better than seeking a posthuman morality that would probably be suitable or functional only in man-made systems which pay less attention to human sentiment or human standards.
Living in a virtual world without such values, as Hernandez argues, we would only "end in despair because it promises advancement but cannot provide escape"(86). Regardless of many reservations we may have on Aristotelian contemplations, we could still argue in favor of the claim that virtue is a skill which requires constant practice. Practically, what would happen next, as Brown argues, depends on our ability to ‘shed old beliefs’.

Thus promoting posthumanism as a philosophy of survival, we could develop a new continuum of ethics and avoid dogmatic rearrangements while doing so. We could eschew ages-old dualism and avoid mythical outdated contradictions. Without confining ourselves to pre-existing templates and straightforward motives, we could systematically eradicate racism and search new ways for self-creation.

Participating in a posthuman mode of thought, we could recognize this thin line between manipulation and enhancement and avoid different posthuman scenarios for extinction. Once we manage to embrace such changes, we would start treating intelligent systems; synthetics or quantum computers as our new born babies and bring them into our ethical and legal consideration to ensure humanity’s survival.

Still being optimistic about our built-in instincts for survival and our ability to establish a healthy social-connection, Brown in all his novels urges humanity to pay much attention to lawsuits that need to be filled. Crucially, for brown even if we made every aspect in life obsolete we must not make our ethics obsolete. We must not commit the same mistake Tankado did with NSA’s databank. And we surely must not leave this particular question: "who will guard the guardians? "(237), then, without a suitable answer.
Works Cited