IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. V (May - June 2017), PP 28-36
www.iosrjournals.org

An Investigation into Ipredation in Cyberspace towards Developing a Framework for Preventing Ipredators' Attacks

Ambrose Kinyanjui Muchonjo[1], Prof. Gregory Wanyembi[2], Dr. Cyrus Makori[3]
[1, 2, 3] *Mount Kenya University,*

Abstract: The information age society is becoming highly dependent on technological advancements and in particular software platform and devices that can access the cyberspace. The way people acquire, access and share data, files and, information have significantly revolutionized peoples' social-technical interactions shaping their lifestyle and activities in regard to both the physical space and cyberspace. Ubiquitous computing for instance tends to offer digital society great, exciting, powerful features and capabilities that enable reliable and productive encounters within convenient environments. In ubiquitous environments however, there is high possibility of users' data, files and other users' digital assets being exposed to high risk of disclosure and tampering by iPredators. Such disclosure and tampering of users' sensitive data and information potentially exposes the targeted persons in society to many risks in regard to their digital and environmental security and privacy. In event of a successful iPredator's attacks on targets, the aftermath tend to be quite devastating sometimes leading to loss of lives, financial investments, critical data, human dignity and/or freedom. Dangers lurking in the cyberspace where there is increased usage of ICTs within a highly connected society of people and devices are therefore real and costly. The iPredators attack on users in cyberspace is a problem that requires cyber security awareness for users to address. To achieve this, this paper explored the various typologies of iPredators attacks targeting users in the cyberspace. The output of the study lead to a proposed framework by the researcher for preventing iPredators attacks on cyberspace. Desktop study research technique was adopted by the study which inclined to qualitative research design.
Keywords: iPredator, iPredation, cyberspace, attacks prevention

I. INTRODUCTION

1.1 Background to the Study

The information age society is becoming more technologically advanced and highly dependent on the ICTs and cyberspace for their daily living activities. Alexander (2012) advancing the same idea argues that the cyberspace is directly impacting upon every area of human endeavor from economic to social, to peoples' cultural and political developments. Nuccitelli (2013) agreeing with this argument observes that technological advancements have indeed changed the way humanity interacts, exchanges and accesses information in both social-political and economic setups. Consequently, iPhones, tablets, smart phones, mobile devices, iPads, chartrooms and social media technologies are advancing at a great pace and gaining great popularity amongst the vast majority of the digital society. However, the high dependence on digital technology also tends to drag the unwitting members of the society into a false sense of trust and reliance on technology. Consequently, large number of people ends up taking information and 'connection' to others in the cyberspace at face value. This creates a security gap whereby new avenues and frontiers for possible misuse of ICTs and the cyberspace are therefore being created each day posing real threats and dangers to members of the society.

For instance, Kimuyu (2017) reported how a Russian by the name Philipp Budeikin invented a suicidal online game by the name Blue whale Challenge in which targets mainly teens are recruited to take part in the deadly online game. The online game involves lengthy brainwashing of targets over a period of fifty days in which targets assigned the so called administrators are assigned dangerous tasks to undertake including the targets asked to inflict on themselves bodily pain and harm while also being forced to isolate themselves from the rest of the society members. Eventually once physically, mentally, psychologically and emotionally exhausted and with little power to make logical decision, the victims are led into committing suicide. Through the game hundreds of teenagers across the world are reported to have committed suicide including one teenager in Nairobi, Kenya which forced the Kenyan authorities to ban the game in Kenya (Kimuyu, 2017). The acts of Philipp Budeikin fit the characteristics of an iPredator. An iPredator refers to any person(s), group or organisation or state engaging in exploitation, victimization, stalking, theft and disparagement of targets or involved in criminal, coercive, deviant or abusive behaviors using ICTs and the cyberspace (Nucitelli, 2013). The iPredator may be cyber criminal, a cyberbully, cyberstalker, cyber harasser, online sexual predator, cyber terrorist, internet troll, online child pornography consumer or distributor or one engaged in internet defamation or nefarious cyber deception.

Jaishankar (2008) further observes that cyberspace is presenting an exciting new frontier for criminologists while easily facilitating new forms of online deviance, crime, and social control. For instance, in Kenyan context such was once identified with Rachael Shebesh the current Nairobi County women's representative who once reported to ISP News agencies how on several occassions while using the internet she got targeted with online harassments by local iPredators on basis of her political ideologies and stand. The accounts given revealed how Shebesh repeatedly endured demeaning attacks suggesting that she is a feminist not fit for leadership while also receiving numerous comments on social media sites full of sexual innuendo forcing her 'keep off social media' in particular (Njagi, 2014). Such iPredatory behaviour by users online against others online contributes to real online distress to victims of the online attacks. At aggravated levels as in the case of victims of Blue whale challenge lives are lost and peace and security within the society threatened. Inter Press Service.

Similar cases of how peace and security of individuals can be threatened by iPredatory behaviour was revealed in Kenya by Sakina (2016) who reported how one Larry Madowo a popular Kenyan TV presenter had suffered real threatening moments occasioned by cyber bullies who viciously targeted him with insults on Twitter for allegedly 'disrespecting' Raila Odinga, the Kenyan former prime minister. Reportedly the nature of comments Madowo was receiving online were so vicious and life threatening that he had to record a statement with the police fearing for his life. However, according to Njagi (2014), Kenya's office of the Director of Public Prosecutions acknowledges that most victims of cyber crime and bullying very rarely report the crime.

In Kandara sub-county of Muranga County, the results of study by Kamaku and Mberia (2014) relating to influence of Social media on prevalence of sexual harassment amongst teenagers revealed that cyberbullying, sexting, online grooming, online sexual solicitations and online sexual predation targeting teenagers was already an online threat problem facing the society. Such online behaviour by iPredators against targets has the potential to present real dangers and risks threatening security and safety of the targeted persons in the society and hence the peace due to harm and damage that results to the persons affected.

1.2 Problem Statement

Dangers lurk in the cyberspace along with increased usage of ICTs within a highly connected society of people and devices. Olowu (2009), Nuccitelli (2013) and Kamaku and Mberia(2014) observes that iPredation is a real threat to persons in the realm of the cyberspace especially much so in a vastly networked society of people and devices. Furthermore, the iPredators often capitalize on the numerous benefits the ICTs and cyberspace offers every user such as anonymity and accessibility to massive data thereby turning these tools and technologies into weapons to deceive, offend, dominate, control, molest, exploit or steal from their intended targets. In addition, any ICT user whenever in the realm of cyberspace is a possible target for iPredators. To address the challenge of iPredation as a risk factor to security and safety of people highly dependent on digital technologies and cyberspace, this paper seeks to propose a model for promoting digital safety and internet security in end users against iPredation for safe use of digital technology and the cyberspace.

1.3 Rationale

ICTs as tools have many different purposes that are highly beneficial to the society in the contemporary world. However when in hands of iPredators or when chosen for malicious reasons, ICTs and the Internet are tools that are now being turned into weapons of attack with great potential to cause real harm to the intended targets, their digital assets, networks. Olowu (2009) while supporting similar view point also argues that it is utter futile for anyone to think that they are immune to cyber attacks all people now inhabit an increasingly connected world. As such, it really does not matter where one lives or who one is as reality and the law of probability dictates that every one of us will get affected at one point in normal routine life.

As the Kenya ICT Masterplan (2014) also observes, the cyberspace has a global outreach and its impacts accelerates beyond national boundaries hence creating quite a complex cyberspace security challenge for any government to address alone. Worthwhile to note too is the fact that online content and activities is mainly user-driven and as such, this requires users to remain more accountable for their personal well-being while online. It is therefore critical for Internet and ICTs users to understand that individual activities and conduct while using various technologies in realm of cyberspace greatly influence whether their online experiences ends up positive or negative upon them and other users as well. Consequently, this paper proposes a framework for dealing with iPredation attempts on users in order to prevent and to stop victimization while minimizing the harm initially intended by the iPredator.

II. LITERATURE REVIEW

2.1 Theoretical framework

The study adopted the space transition theory. According to Jaishankar (2008), the traditional theories of criminal behaviour are not fully sufficient in explaining criminal activities on the cyberspace since as cyber

crimes and other online offences are different from criminal activities on the physical space. Jaishankar (2008) explains that the Space Transition Theory is an explanation about the nature of the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and cyberspace. This captures clearly the dynamics of activities involving motivated digital abuser and a vulnerable digital victim in realm of the cyberspace leading to thriving iPredation. Moreover, people tend to behave contrary to their true self while on cyberspace as compared to when they are on the physical space resulting likelihood of iPredation cases on the cyberspace.

2.2 The 5 iPreV Model

Based on Nuccitelli (2013) ideas of iPredator construct, this study proposes a **5 iPreV** theoretical model of iPredation to conceptualize digital abuser and digital victim dynamics and all social interactions between people who routinely use ICTs in the realm of cyberspace. Cyberspace or online users can be viewed in terms of ICT intents, actions or motivations and therefore online experiences on users are likely to be impacted upon by the various content driven activities by the targets themselves as well as other ICTs users in the realm of cyberspace. The 5iPreV theoretical model is a representation of the five elements involved in all ICTs, cyberspace and the criminal deviant or abusive interactions between online users. These elements include the iPrey, iPredator, iVictim, iPrevention and the iPreservation. The major difference between the 5 iPreV framework and other criminal and deviant victimization dynamics is the Cyberspace which creates an environment in which the digital offender and victim interact. Arguably, the cyberspace tends to benefit the iPredator in presence of ICTs users who lacks appropriate digital skills and ethics to deflect iPredator attacks.

2.3 Typologies of iPredation in cyberspace

As mentioned earlier, an iPredator may be a cyber criminal, a cyberbully, cyberstalker, cyberharasser, online sexual predator, cyber terrorist, internet troll, online child pornography consumer or distributor or one engaged in internet defamation or nefarious cyber deception. These typologies of iPredators are discussed briefly under this sub section.

Cyberbullying as a term may refer to minors using ICTs to humiliate, taunt, insult, embarrass and disparage one another mainly intending to damage the target's environmental and digital reputation while inflicting great emotional and psychological distress on the victim. However the term may have varying meaning depending in context and environment it is being used. For instance cyberbullying may also involve adults using various ICTs and social networking technologies while targeting others online. Cyberbullying can be perpetrated in different ways by an iPredator including: (1) Flaming which involves sending messages that are rude or vulgar in nature about a person via an online group, e-mail, or instant/text message, (2) Outing which refers to posting or sending content about a person that is sensitive and/or private, (3) Exclusion which is deliberately and cruelly excluding someone from an online group, (4) Denigrating which involve sending or posting untrue and cruel statements about a particular person. This can include e-mail or text insults about another person's physical characteristics, such as looks or weight, and (5) Masquerading which refers to posing as someone else for the purpose of sending information via the Internet that makes that individual look bad after the target security has been compromised for instance through stolen passwords allowing access to target's computers or cell phones.

Cyberstalking is a typology of iPredation that refers to the use of ICTs to stalk, control, manipulate or habitually threaten a child, adult, business or group with direct or implied threats of physical harm. This is characterized with habitual surveillance and gathering information to manipulate and control a target. Moreover, ICTs may be employed to issue variety of threats against the intended victim(s) including: disparagement, humiliation, disinformation, dissemination and damage to the target's digital and environmental reputation, credibility or financial status (Nuccitelli, 2013). Cyberharassment on the other hand is the use of ICTs to harass, control, manipulate or habitually disparage a child, adult, business or group without a direct or implied threat of physical harm. Cyberharassment mainly involve the use of ICTs to execute verbal, sexual, emotional or social abuse against a person, group or organization while aiming to exert power or exercise control over the targeted victims.

Cyber Terrorism involve use of ICTs by organized groups or terrorist groups[iPredators] while advancing their malicious agenda targeting victims mainly for religious, political or philosophical ideologies and other related gratifications. Accordingly, cyber terrorism activities may include: (1) The use of ICT to organize and execute attacks against networks, Information, ICT infrastructures etc, (2) The exchanging of information or making threats electronically, (3) The act of hacking into computer systems, Introducing viruses and malware to vulnerable networks, (4) Defacement of websites and blogs, Denial-of-Service Attacks, and (5) Terrorist threats made via electronic communication.

Online sexual predator is mainly an adult online user bent on using various ICT platforms to exploit vulnerable persons for sexual and other abusive purposes. Using the ICTs and the Internet online predators are

able to locate, target, engage and victimize their intended targets mainly after carefully planned online grooming and online sexual solicitation (Nuccitelli, 2013). Most of the cases, the online predators tend to use the same ICTs to cheaply and easily produce unlawful pornographic materials for distribution either online or by streaming the sexual videos live using webcam enabled digital devices for financial gains and personal gratifications. Various online forums may be used by online Predators to target the potential victims including: chat rooms, instant messaging or even social networking sites.

Sexting as a typology of iPredation refers to people taking nude or sexual or sexually provocative images either using still or video camera enabled digital device such as a cell phone and then sharing such materials using various digital platforms. Aftab (2012) also argues that the term sexting may also include taking and sharing of sexual or nude images or video, no matter what device was used to shoot them. Moreover, 'cybering' which refers graphic sexual discussions differs from 'sexting' in the sense that they refers to images and videos being used to communicate in sexually provocative way (Aftab,2012).Accordingly Sextists usually take pictures and videos of themselves in sexually provocative poses, while nude or partially nude engaging in sexual activities either real or posed intended for later electronic sharing. Other typologies of iPredation involves: Cyber Hate, Online grooming and solicitations, Identity theft, online fraud, Sextotion, online sex tourism and many more both existing and emerging typologies and forms of iPredation.

2.2 Conceptual Framework

The main variables are the targets (iPrey & iVictims), the iPredators, iPredation attacks in cyberspace and the Digital Self defense strategies (iPrevention & iPreservation) for addressing the cyberspace security threats and risks due to iPredators presence in cyberspace.

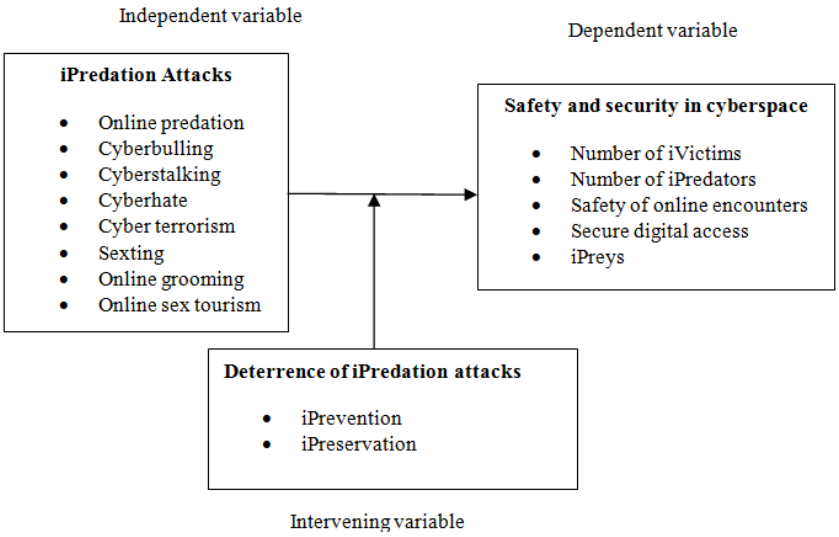

Figure 1: Conceptual Framework

III. RESEARCH METHODOLOGY

3.1 Research Design

This study adopted a qualitative research design which was intended to help the researcher explain the unique interactions in a particular situation in order to understand in depth, the characteristics of the situation and the meaning brought about by participants and what was happening to them at the moment (Patton, 2002). Through the qualitative research design, the researcher also sought to gain new insights, and discover new ideas while also seeking to increase knowledge regarding the phenomenon of iPredators and social engineering attacks (Mason, 2002).

3.2 Research Technique

Research technique as a term refers to the behaviour and instruments the researcher would use while carrying out research operations such as recording data, techniques of processing data as well as making observations (Kothari, 2004). This research adopted the desktop study technique for acquiring relevant information regarding the phenomena of iPredation in cyberspace and how it affects online and digital security and safety of the affected persons in the society and therefore the peace within any given environment in a society. Desktop study is defined by Management Study Guide (MSG, 2014) as a research technique whereby the researcher is able to access and collect data faster and cheaply from pre-existing resources. Moreover, according to Paul (2005) desktop research refers to a research technique in which secondary data is gathered

from pre-existing sources. These data sources includes: (i)library data such as journals, newspapers, reports, government reports, EU statistics, industry statistics, technical papers,or white papers (ii) Internal data within organisations, and (iii) Internet data such as statistics or company websites (Paul, 2005).

IV. FURTHER DISCUSSION

4.1 Digital Mediums for Online Bullying, Stalking and Harassments

There are many different forms of digital mediums that are used to bully, stalk or harass intended targets. These media and technologies platforms may include: (1) E-mails: It is a form of electronic communication involving the transmission of messages over the Internet: Online assaults to a target can occur when inappropriate messages, photos, pornography, or computer viruses are e-mailed to the victim, (2) Chartroom: it is a virtual community in which a group of individuals "dialogue" and share information with each other asynchronously (Nuccitelli, 2013). A perpetrator can use this forum to spread rumors or negative or damaging report or personal information about a victim to the group, (3) blogs. These are similar to website journals where entries might include commentary, information about events, graphics, videos, or images, all of which are posted by an individual and viewed in chronological order. Cyberbullying, Cyberstalking and Cyberharassment occur when an individual posts negative, private, damaging and/or false information about the victim while encouraging others to enter the blog to read the commentaries. The aim is to damage the target's credibility, digital and environmental reputation, (4) Instant Messaging and text messaging: These are forms of synchronous communication whereby individuals communicate through text using computers or other devices, such as phones, and (5) Social networking technologies and websites: A cyber bully or cyberstalker can easily create pages with threatening, damaging or hurtful information about a victim on a specific website.

4.2 The Offline Distress Dictates Online Response (ODDOR) Theoretical Construct

The ODDOR construct by Nuccitelli (2013) proposes that an ICT user's offline environmental distress and pressures directly affects to how they behave online. This argument is helpful in understanding the need for ICT users to effectively institute iPrevention while on the cyberspace to effectively deflect iPredators. As Nuccitelli (2013) observes, pressures and frustrations from home, school, work, finances etc may tend to bring significant pressure and distress to an individual. Under such circumstances, research has shown that such an ICT user is more likely to be less vigilant in their Internet safety tactics and therefore more likely to engage in high risk online behaviors. This makes them most vulnerable to iPredator attacks while on the cyberspace. Moreover, under the concept of D4 (Distracted, distressed, discouraged or dysfunctional), users who have been highly stressed and distressed offline makes most favourable profiles and choice targets for iPredator. The victims who fell prey to the Blue whale challenge game for instance are classification that fit the characteristics relating to the ODDOR construct in iPredation dynamics.

4.3 Notable iPredatory Attacks and behaviour in Kenya in recent past

This section will discuss typical and notable stories involving cyber abuses, online bullying and other forms of iPredator attacks happening amongst Kenyan digital society alongside the outside world experiences. It is worth noting here that Kenya lacks proper legislation to police cyber crime as reported by the BusinessDailyAfrica (2013) which argued that Kenya's cyber security is one of the weakest in the world to an extent that IT savvies can easily intercept [mobile phone] voice traffic and obtain temporary secret keys for some subscribers. This observation is clearly demonstrated from some of the accounts of online incidence and activities involving our digital community as following discussions clearly depicts.

4.3.1 #KenyaVsZimbabwe: Twitter War

Twitter War(TWar) erupted from Kenyan social media users following an apparently fabricated publication published on November 3, 2015 by a Kenyan blog claiming that Zimbabwe's President Mugabe insulted Kenyans labeling them "the most arrogant thieves in the world with wizardry in stealing while also insinuating that Kenyan universities must be as well be offering Bachelors in Stealing and as such warning Zimbabweans to be on high alert whenever around any Kenyan lest they contract the same 'disease'. The Spector.co.ke had apparently published the story in the article; God Should never have created those thieves (Kenyans) here in Africa. The short article apparently triggered cyberhate and consistent online attacks on Zimbabwe and Zimbabweans (Exponent, 2015). This was arguably executed by Kenyans on Twitter (KOT), apparently a Digital Community reacting to Mugabe's insults and contempt on Kenyans. On November 4, 2015, NYT's Bureau Chief for East Africa, Jeffrey Gettleman supposedly published an article titled; An Anticorruption Plea in Kenya: 'Please, Just Steal a Little'. This article apparently claimed a heightened level of corruption affecting Kenya while again reportedly inserting within the article the same 'remarks from the Spectator' supposedly without proper verification and authentication of the source only for the claim to be taken

back later (Gentleman, 2015).Apparently Jeffrey Gentleman owned up the mistake and apologized through twitter to all affected by his misleading article.

4.3.2 Distribution of Disturbing images of Slain KDF soldiers in Somalia

A number of Kenyan bloggers and Whatsapp users got arrested for an alleged number of offences ranging from posting disturbing images of slain KDF soldiers, to posting unlawful tweets (Sakina, 2016). This online exposure of slain soldiers though meant to show solidarity with families of the victims of the unfortunate attack on KDF soldiers in Somalia by Al Shabab terrorists also in a way promoted publicity for the attackers and indirectly their cyber terrorist activities while inflicting untold pain and distress to families of the victims of the attack.

4.3.3 #MyDressMyChoice debate and Distribution of indecent videos of stripping of women

According to Sakina (2016) women were stripped in public by large groups of men for being 'indecent' with Videos of the stripping going viral on social media platforms like Facebook and Twitter as well as Whatsapp groups. Such acts by those involved in sharing those digital contents and communications only left the victims captured in those videos with more psychological trauma and shame especially much so that many people probably saw the videos.

4.3.4 The Offensive Tagging of Pornographic materials on targets' walls

According to Sakina (2016), ICT users are being tagged in pornographic material in the form of a link, video or picture mostly on their social media platforms. This has become disturbingly very common with real potential of damaging the environmental and digital reputation of the targeted victim. More often the victims of such online assaults only get to know of such incidences from others. Moreover, with large personal information available in the public domain, hackers can easily hack the victim's account, con people, spread malware or just be downright malicious and spoil the victim's name and digital reputation. Such are acts of iPredation being perpetrated through ICTs as weapon of attack.

V. THE FRAMEWORK FOR ADDRESSING THE CHALLENGE OF IPREDATION IN CYBERSPACE

This paper proposes the iPrevention and iPreservation framework for digital and cyber self-defense against the iPredatory attacks in cyberspace.

5.1 iPrevention and iPreservation framework for digital self defense

The law of probability argue that all users will be confronted with some form of online attack by iPredators at one point in their life (Olowu, 2008); (Nuccitelli, 2013). Social engineering techniques are choice approaches that iPredators employs while planning and executing attacks against targets and therefore the way the target handles digital technologies or behaves online becomes critical in deflecting possible attacks. This framework recommends that all end users diligently practice effective iPrevention as the primary step of reducing the probability of being targeted with social engineering attacks.

Under the concept of iPrevention every digital and cyber user must remain conscious of the need to observe cyber ethics, cybersafety, and cybersecurity (C3) practices to ensure their personal digital safety and the security of their digital assets while in realm of cyberspace. By diligently observing iPrevention, the target actually is involved in efforts of denying the iPredator(s) the benefit or reward that they would have gained by successfully executing the attacks. Moreover, through iPrevention, the target(s) tends to increase risks on part of the iPredator thereby discouraging the iPredator activities in the cyberspace.

Consequently iPrevention constitutes to target's digital self defense mechanism against attempts of social engineering attacks and hence increasing their potential of deflecting social engineering attacks targeted on them. To effectively deflect most digital attacks including social engineering attacks, iPrevention must therefore remain a cybersecurity and cybersafety skill to be constantly learnt and to be diligently practiced by all digital users. On the other hand, iPreservation as attacks deflection mechanism simply implies that all digital and cyber users diligently ascribe to the practice of instituting iPrevention against potential cyber attacks including social engineering attacks. According to Nuccitelli (2013) iPreservation is an innate state of self-survival manifesting in end users whenever interacting via digital devices or participating in cyber activities for social, business purposes or otherwise. Consequently, the practice of iPreservation therefore serve to trigger appropriate internal responses in human targets prompting them to act accordingly and appropriately to shield themselves from any possible digital or cyber attacks such as the iPredators' social engineering attacks.

Digital self defense therefore results from users carefully observing sustained levels of iPrevention and iPreservation practices that require all end users to diligently observe security best practices and controls for

deflecting attacks at personal level. This may include upholding best security practices while using ICTs and observing digital and Internet safety at all times. Some of these practices are described below.

5.1.1 Adopting Craigslist for Online Safety

Aftab (2012) recommends Craigslist Safety tips to be adopted by all online users while using the cyberspace to enhance their safety while online for gainful use of the cyberspace. This study also seeks to encourage the adoption of similar online safety tips by our Kenyan online users to minimize chances of victimization by iPredators during online encounters. These Safety tips according to Aftab (2012) include:

1. Use of trusted sites, doing comparison shopping, "Google search" the company, website, person, address, email, contact information and product.
2. Phone a friend and ensure one is running the deal or encounter with someone he/she know and trust.
3. Do it in public for it is much safer when others are around.
4. Keep a record. Print everything out including the ad, the email chain, pictures, directions, names and addresses. Save voicemails and texts.

5.1.2 Adopting Craigslist Tips for online Dating

This study proposes the following Craigslist Tips for safer online dating as recommended by Aftab (2012) for ensuring safer dating encounters online. These include:

I. Treating the first "real life" encounter as a first and blind date and bringing a friend to meet in a public place.
II. Being honest and demand honesty. Find background and marital status where possible from the Cyberdating sites
III. Just leave the place, end the communication or unfriend the person if things don't work out as expected.
IV. Avoid sharing personal info too early to guard your privacy. Use Craigslist's email anonymizer instead of sharing the real email with anyone online.

5.1.3 Adopting Parry Aftab's cybersafety 1-2-3 approach for Households

Aftab (2012) proposes "a 1-2-3 approach to cybersafety" involving three steps to be adopted by households in efforts to ensure safer household use of the cyberspace. This study also proposes adoption of a similar 1-2-3 approach to cybersafety to insulate our Kenyan households against various forms of iPredator attacks. Aftab (2012) suggests that this cybersafety approach requires the family head(s) to take an inventory of existing devices and connected technologies and to help survey the needs and ability to allocate time to the issues and secondly ensure that rules are determined, set and then communicated to the children and caregivers. Thirdly and finally is to ensure that these rules are enforced within the bounds of the household (Ibid).

5.1.4 Diligent Awareness by ICTs users on potential Spyware attacks and surveillance threats

There are several different kinds of technologies that can be "used to 'spy' on ICT users either through their computers or other digital devices. This includes the various computer programs, mobile application programs and commercial applications such as the 'keystroke loggers' that reports back to the person who sent it with everything one type, including passwords, login information, pictures, posts, emails, instant messages, chat logs and credit card numbers. Furthermore, Trojan horses can also be used in spying by giving attacking party access to the intended target's computer or mobile device through remote control, allowing them to access everything the target have on their hard drive or digital hand set (Aftab, 2012). Consequently the iPredator is able to gain control of the targets' webcam and audio recording technologies. This allows the iPredator or the malicious code to add harmful contents, erases files, and even reaches out to anyone on the target's contact list for malicious reasons. Consequently, Aftab (2012) suggests that a good security suite by a well-known security software provider is helpful in identifying and removing majority of the spywares. The ICT users should also frequently use updated antivirus software definitions at all times in their computers, laptops, tablets, iPads, iPhones and smart phones to keep them free from malwares, adwares and spywares which are the major sources of privacy and security threats of digital assets.

5.1.5 Diligent Handling and Use of Passwords

Passwords should always be used to lock the computer when one is not sitting at the keyboard since anybody can secretly access it and install spyware (Aftab, 2012). It is worth noting that cell phones, smart phones and other handheld devices often permit one to set a password or a "lock code" that will prevent unauthorized access to one's contacts, photos, reading personal messages from unattended personal phones and portable digital devices etc (Ibid).

5.1.6 Understanding and Handling Privacy Settings

Aftab (2012) observes that online assailants (iPredators) can indeed be stopped from harassing ICT users or being able to contact them by adjusting privacy, security and personal settings on any digital device or application programs running on them to increase their privacy and security where need be. Consequently, it is possible to limit the people allowed to see one's profile, pics or personal information. For instance Facebook's privacy settings (facebook.com/privacy) have a feature which allows users to even block certain people or accounts. These privacy settings also include those which allow users to execute commands to "ignore, block sender or block specific people etc". Others settings can also limit communication to everyone except for those one wish to hear from (Aftab, 2012). Moreover most social media platforms, instant messaging software, application programs etc has an online reporting mechanisms where users can report a bad experience with their product for necessary action.

5.1.7 Setting one's Google Alerts

According to Aftab (2012), one ought to learn how to 'Google' themselves. Equally important for online users is too often do some search for their whole name, search for their cell number, screen names and email addresses, search for their nicknames and home address and then set a Google Alert that will be sending them an email any time Google finds this information online (Aftab,2012). Consequently, "the sooner the online user know about something that is posted about them that shouldn't be, the faster they will respond appropriately to avert the intend harm.

5.1.8 Securing all Mobile Computing and communication devices

Aftab (2012) observes that the likelihood of a malicious person grabbing unattended portable devices and mobile phones are high especially with intents to maliciously change settings, forwarding private images or texts while posing as the cell phone owner when harassing others. Moreover, Aftab (2012) discussing a survey by WiredSafety had teens reporting more than seventy different ways they can use a cell phone to cyberbully others. Moreover, anyone with malicious intents is capable of doing anything with unattended and unprotected digital computing and communication devices intending to have their victim take the blame on it (Aftab, 2012). Moreover, it is important to be aware that spyware are easily installed on an unattended and open device, much as GPS features for surveillance and monitoring of intended victim can and therefore strict care should be taken to keep such devices away from unauthorized persons (Ibid).

VI. Recommendations

The study recommends that specific study be done in line with the emerging cybersecurity threats by unique typologies of iPredatory attacks in cyberspace to come up with customized frameworks and solutions against the ever evolving challenge of iPredation along with high reliance of ICTs by the information age society within the highly connected environments of people, networks and information communication devices.

A recommendation is also made for stakeholders such as schools and school administrators, parents and guardians, government agencies and general public at large to consider adopting the framework proposed by this study to enhance the digital and cyber safety of the people under their mandate or within their environments in order to promote secure digital access of cyberspace with reduced threats and victimizations by iPredators prowling in cyberspace.

VII. Conclusion and Research Gaps

The paper managed to explore the various typologies of iPredators attacks targeting users in the cyberspace as well as the choice digital platforms by iPredators for executing the various forms of iPredatory attacks against the choice targets. Moreover the paper highlighted on the ODDOR construct as an explanation of what unique characteristics in a targets that make for choice targets for iPredation. Furthermore, the paper highlighted on notable cases that comprised iPredation within digital society and the Kenyan cyberspace. The output of the study lead to a proposed framework by the researcher for preventing iPredators attacks on cyberspace. The study did not restrict itself to any specific typology of iPredation attacks in cyberspace. Further research ought to be carried out on specific typologies such as: Social engineering attacks, Ransomware attacks, online bullying, Malware attacks and even cyberterrorism as well as studies leading to solution for addressing the unique cyber security threats challenges and risks due to iPredatory attacks in cyberspace whether technical, social-technical or otherwise.

REFERENCES

[1]. Aftab,P. Wired Safety (2012) Wired Safety Resources on cyberbullying, cyberstalking, sexting and Internet safety. Retrieved June 28th 2015 from http://www.wiredsafety.org and http://www.aftab.com

[2]. Alexander K. (2012). National Cyber Security Framework Manual. Pretoria: Van Schaik Publishers.

[3]. BusinessDailyAfrica (2013). businessdailyafrica.com. Retrieved March 16th, 2016, from www.businessdailyafrica.com/Corporate-News: http://www.businessdailyafrica.com/Corporate-News/Experts-fault-Kenya-s-cyber-security-after-18-month-test/-/539550/2083724/-/61begg/-/index.html

[4]. Georgia Tech Information Security Centre, (2008). Emerging Cyber Threats Gibson, W. (1984). Neuromancer New York, NY: HarperCollins.

[5]. Gentleman, J. (2015, November 4). www.nytimes.com. Retrieved March 15, 2016, from nytimes.com: http://www.nytimes.com/2015/11/05/world/africa/kenya-government-corruption.html?_r=0

[6]. Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

[7]. Kamaku, M. N., & Mberia, H. D. (2014, April). The Influence of Social Media on Prevalence of Sexual Harassments among Teenagers. International Journal of Academic Research in Business and Social Sciences .

[8]. Kemper, E., Stringfield. S., & Teddlie, C. (2003). Mixed methods sampling strategies in social science research. In A. Tashakkori & C. Teddlie (Eds.), Handbook of mixed methods in social & behavioral research (pp. 273-296). Thousand Oaks, CA: Sage.

[9]. Kimuyu, H. (2017, May 12). nairobinews.nation.co.ke. Retrieved May 14, 20, from nation.co.ke: http://nairobinews.nation.co.ke/life/man-behind-online-game-drove-kenyan-teen-commit-suicide-pleads-guilty/

[10]. Kothari, C. R. (2004). Research Methodology: Methods & Techniques. New Delhi: New Age International (P) Ltd.

[11]. Mason, J. (2002). Qualitative researching (2nd ed.). London: Sage.

[12]. MSG. (2014, July 14). managementstudyguide.com. Retrieved August 17, 2016, from Management Study Guide: https://www.managementstudyguide.com/desk-research.htm

[13]. Nuccitelli, M. D. (2013, June). iPredator. Retrieved May 7, 2015, from www.ipredator.co: https://www.ipredator.co/cybercriminal-5pv-model/

[14]. Nuccitelli, M. D. (2013). iPredator-Global Internet predator Theory. Academia

[15]. Nuccitelli, M. D. (2013, June). iPredator. Retrieved May 7, 2015, from www.ipredator.co: https://www.ipredator.co/cybercriminal-5pv-model/

[16]. Nuccitelli, M. D. (2013). iPredator-Global Internet predator Theory. Academia , 31.

[17]. Olowu, D.,(2009). 'Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa', 2009(1) Journal of Information, Law & Technology (JILT

[18]. Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). Thousand Oaks, CA:

[19]. Public Safety and Homeland Security Bureau (n.d) ,'Tech Topic 20: Cyber Security and Communications.' FCC, http://transition.fcc.gov/pshs/techtopics/techtopics20.html

[20]. Ribble, M. S., Bailey, G. D., & Ross, T. W. (2004). Digital Citizenship-Addressing Appropriate Technological Behaviour. International Society For Technology in Education , 6.

[21]. The Kenya National ICT Masterplan (2014). Government Printer; Nairobi.Retrieve from http://www.ict.go.ke/docs/MasterPlan2017.pdf on 27th June 2015.

[22]. Sakina, M. (2016, February 2).The good, the bad and the ugly of social media [blog post]. Retrieved from http://www.hapakenya.com/author/sakina/ on February 22, 2016

[23]. Spector.co.ke. (2015, November 5th). God should never have created those thieves here in Africa. Retrieved March 15th, 2016, from Spector.co.ke: http://www.spectator.co.ke/2015/11/robert-mugabe-god-should-never-have-created-those-thieves-kenyans-here-in-africa/Republic of Kenya, (2012). Sector for Quarter Statistics Retrieved on June 13th 2015 from http://www.cck.go.ke/resc/downloads/Sector_statistics_for_Quarter_2_-_2012-2013.pdf

[24]. The African exponent (2016, February 22). #KenyaVsZimbabwe: Kenya's Cyber-Bullying Tactic and Misguided Twitter Tirade[blog post].Retrieved from http://greatzimtraveller.com/ on November 8, 2015