

# **iPredator- A Global Internet Predator Theory**



**2012**

**Michael Nuccitelli Psy.D., C.F.C.  
NYS Licensed Psychologist  
iPredator Inc.**

[www.iPredator.co](http://www.iPredator.co)

## TABLE OF CONTENTS

<b>iPredator Definition</b>	<b>3-19</b>
<b>5PV Model</b>	<b>19-25</b>
<b>iPredator Behavioral Categories</b>	<b>26-29</b>
<b>Internet Safety Factors</b>	<b>30-41</b>
<b>5PV Model Notes</b>	<b>41-46</b>
<b>Note to Readers</b>	<b>47</b>
<b>iPredator Inc.</b>	<b>48-49</b>
<b>Resource Links</b>	<b>50-53</b>



# iPREDATOR



As a forensic psychologist with expertise in theoretical criminology and abnormal psychology, I have formulated a psychological, sociological & criminological construct for the growing dimension known as cyberspace. In the manuscript that follows, I introduce my theoretical paradigm and profile, iPredator, who I believe to be the modern-day criminal and psychological reprobate. This new breed of human predator uses Information and Communications Technology to profile, locate, track and attack their prey. The typologies of iPredator include: [Cyber Bullies](#), [Cyber Stalkers](#), [Cyber Criminals](#), [Online Child Predators](#), [Cyber Terrorists](#) and anyone who uses Information and Communications Technology and the Internet to harm online users or engage in deviant and/or bizarre behaviors.

The term, iPredator, is a global construct designed to include any child, adult or organized group who uses [Information and Communications Technology](#) & the Internet to harm, abuse, steal from, assault or engage in malevolent or nefarious activities against other Information and Communications Technology users. This writer and his colleagues recognize this construct is a "work in progress" and will be amended accordingly with the advancement of information technology. Given the rapid progress of technology and the increasing reliance society has, the construct of iPredator and all its sub-constructs should be considered liquid. These terms and their theoretical structures will be intermittently amended as society and information technology becomes increasingly interdependent. Development of the iPredator constructs relied upon information from multiple sources, but the [United States Federal Bureau of Investigations](#) (FBI) is credited as being the a priori resource.

iPredator is a concept to be used by all private and public sector professionals in their endeavors to educate the community, investigate nefarious online activities and to assist the online community develop Internet Safety and iPredator protection practices. When conducting research on iPredators, it is recommended to always ensure the definition is the most recent. The 2012 formal definition of iPredator is as follows:

**iPredator:** A child, adult or group who engages in the exploitation, victimization, stalking, theft or disparagement of others using Information and Communications Technology (ICT.) iPredators are driven by deviant fantasies, desires for power and control, retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance or personal and financial gain. iPredators can be any age, either gender and not bound by economic status, race or national heritage.



On April 6, 2012, the owner of an Internet service provider in Indiana was charged with blackmailing children into performing sexually explicit acts over a webcam. [Richard Leon Finkbiner](#), age 39, of Brazil, Indiana was charged in a federal complaint with sexual exploitation of children. The allegations involved two 14-year-old boys, but the FBI found thousands of sexually explicit images and videos on Finkbiner's computer that suggested "several hundred" other victims were involved in Finkbiner's scheme of "sextortion."

Using the pseudonym "Josh Swaim," Finkbiner would befriend young boys on social networking sites and capture sexually explicit video of them they had uploaded on anonymous video chat sites. He would then tell them that if they did not record more sexually explicit videos, he would release the clips online or send them to their friends.

Finkbiner was quoted as telling one victim that he was a "[hacker](#)" who knew how to remain anonymous. Analysis of Finkbiner's computer and other digital media uncovered thousands of video files depicting hundreds of individuals in various states of undress or engaged in sexually explicit conduct. Most of these individuals were between the ages of 14-16 years of age. Finkbiner would threaten to make these images available to people close to the victims, which was designed to frighten them. Finkbiner threatened to tell the children's parents, friends and coaches. He also threatened to post their images on gay pornographic websites.

*"Only I have this link," Finkbinder wrote to one victim, asking: "You want to play this game or you want to be a gay porn star?" To another, Finkbinder acknowledged, "Yes it is illegal and I'm ok with that," warning: "If you don't play I promise I'll fuck your life over...I won't get caught I'm a hacker I covered my tracks." The level of terror his threats caused the children were chillingly revealed in the transcript of an email message one of the boys sent to Finkbinder pleading, "All I ask from you is to delete it please I'm only 14, please just do this to somebody else, not me please."*

Prosecutors said the case was an example of [Sextortion](#). Crime authorities define sextortion as iPredators catching victims in embarrassing situations online and threatening to expose them unless they create sexually explicit photos or videos for the iPredator. As of May 2012, the presence of hundreds of victims alleged to have been perpetrated by Richard Leon Finkbinder puts their investigation and prosecution among the larger, if not largest, sextortion case prosecutors have ever undertaken in the United States.

On May 4, 2011, [William Francis Melchert-Dinkel](#) was convicted on two counts of aiding suicide in the death of 32-year-old Mark Drybrough, of Coventry, England, who hanged himself in 2005 and 18-year-old Nadia Kajouji of Brampton, Ontario, who jumped into a frozen river in 2008. State prosecutors presented evidence he posed online as a 28-year-old, depressed female nurse engaged in encouraging, advising and assisting young adults to commit Internet suicide. Melchert-Dinkel frequented suicide chat rooms under the names "Li Dao," "Cami D," and "Falcongirl." He is the first person charged and convicted of assisted suicide using the Internet.

Melchert-Dinkel was obsessed with hanging, suicide and searching out potential suicide victims online. Court documents said Melchert-Dinkel told police he did it for the "*thrill of the chase*." He acknowledged participating in online chats about suicide with an estimated twenty people, entered into felonious suicide pacts with ten and five he believed succeeded. Central to his deviant obsession, Melchert-Dinkel encouraged his victims to stream their suicides live on webcam for him to watch. Sentenced on May 4, 2011, Melchert-Dinkel was given 320 days in jail and for ten years thereafter, incarcerated for two days per year on the anniversaries of the victim's deaths.

In September 2011, The [2011 Norton Cyber Crime Report](#) was released that studied the impact of cyber crime and included a survey of 12,000 adults in 24 countries. The report provided an authoritative and accurate picture of the scope of [cyber crime](#) globally and the results were shocking.

The Norton study calculated the cost of global cyber crime at 114 billion dollars annually. Based on the value victims surveyed placed on time lost due to their cyber crime experiences, an additional 274 billion dollars were lost. With 431 million adult victims at an annual price of 388 billion dollars globally based on

financial losses and time lost, cyber crime cost the world significantly more than the global black market in marijuana, cocaine and heroin combined estimated to be \$288 billion dollars.

According to the Norton Cyber Crime Report, more than 2/3 of online adults (69%) had been a victim of cyber crime in their lifetime. Every second 14 adults became a victim of cyber crime, resulting in more than one million cyber crime victims a day. For the first time, the Norton Cyber Crime Report revealed that 10% of adults had experienced cyber crime on their mobile phone. In fact, the [Symantec Internet Security Threat Report, Volume 16](#) reported there were 42% more mobile vulnerabilities in 2010 compared to the previous year.

With these incredible results, it signified that [cyber criminals](#) were starting to focus their efforts on the mobile device users. The number of reported new mobile operating system vulnerabilities increased, from 115 in 2009 to 163 in 2010. In addition to threats on mobile devices, increased social networking and a lack of protection were considered the main culprits behind the growing number of [cyber crime](#) victims.

On September 22, 2010, [Tyler Clementi](#) (December 19, 1991-September 22, 2010,) an eighteen-year-old student attending Rutgers University in Piscataway, New Jersey, jumped to his death from the George Washington Bridge in New York. His roommate and a fellow hall mate used an [instant messaging](#) software application to view, without Clementi's knowledge, Clementi kissing another man. The roommate later attempted to view Clementi's sexual encounters a second time and drew attention to the event by making Twitter postings to his 150 followers and in private messages to his friends. After discovering that his roommate had secretly used a webcam to stream his romantic interlude with another man over the Internet, he jumped off the George Washington Bridge.

The roommate, who faced fifteen charges, included [invasion of privacy](#), [witness tampering](#), and [evidence tampering](#) with further charges of [bias intimidation](#) attached to some of the basic charges. The roommate was found guilty of all 15 counts on March 16, 2012, including all four bias intimidation charges. He was not charged with a role in the suicide itself. His accomplice was not charged in exchange for testifying against the roommate and doing community service. The suicide of Mr. Clementi focused the United States on the victimization of gay, lesbian, bisexual and transgender youth and the growth and negative impact of [cyber bullying](#). Public figures, including Ellen DeGeneres and President Barack Obama, spoke out about the tragedy and New Jersey legislators enacted the nation's toughest law against bullying and harassment in January 2011.

***"Welcome to the unseemly and perverse world of iPredator."  
Michael Nuccitelli Psy.D., C.F.C. (2011)***



iPredator is a global term used to distinguish all online users who engage in criminal, deviant or abusive behaviors using Information and Communications Technology. Whether the offender is a [cyber bully](#), [cyber stalker](#), [cyber criminal](#), [online sexual predator](#), [Internet troll](#) or [cyber terrorist](#), they fall within the scope of iPredator. There are three criteria used to define an iPredator including:

**I. A self-awareness of causing harm using Information and Communications Technology. II. The intermittent to frequent usage of Information and Communications Technology to obtain, exchange and deliver harmful information. III. A general understanding of Cyberstealth used to profile, identify, locate, stalk and engage a target.**

When an offender profile includes these three characteristics, they meet the definition of iPredator. Of the three measures used to define an iPredator, the first criteria, a self-awareness of causing harm using Information and Communications Technology, can be difficult to confirm unless the online user has personally assessed their own motivations. When others attempt to valueate if someone is an iPredator using factor one, they must use circumstantial evidence leading to the conclusion the online user is aware of the harm they are causing others using Information and Communications Technology.

In relationship to [cyber bullying](#), there is a small percentage of young online users who are either ignorant of the harm they are causing another person or genuinely believe they are joking. Another small sub-group of online offenders not meeting the first criteria are [cyber stalkers](#) who suffer from a verified Axis I psychiatric mental illness (i.e. [Obsessive Compulsive Disorder](#), [Bipolar Disorder](#), [Schizophrenia](#), etc.) Online users who suffer from severe mental health issues may in fact not be aware that their habitual attempts to contact and/or connect with another online user are causing the recipient significant distress. Of the total pool of iPredators at any given time online, this writer estimate 1-3% of them are not aware of the harm they are inflicting upon their victim.

A fourth criterion, not included in the triad defining an iPredator, is what I have termed iPredator Victim Intuition (IVI) and reserved for seasoned iPredators. IVI is the aptitude to sense a target's online vulnerabilities, weaknesses and technological limitations increasing their success with minimal ramifications. iPredators, through practice and learning, develop a sense and/or skill of being able to experience an intuition to know what online user will be a successful target.

Just as classic criminals can "[case](#)" a home or choose the most vulnerable child to abduct, the iPredator is able to do the same using information they compile from a variety of online sources and contacts they may or may not have with a potential victim. Based on the typology of iPredator, the areas they investigate in their strategy of targeting a victim include:

- 1.** The amount of personal information a potential target posts or shares online.
- 2.** The frequency a potential target posts or shares their contact information online.
- 3.** The content of the information a potential target posts or shares online.
- 4.** The lack of Internet safety measures a potential target institutes online.
- 5.** The potential targets willingness to discuss sensitive issues including: sexual topics, financial information, their physical location, parental or adult monitoring of their online activities, experiences of distress at home, work, school and interpersonal or intrapersonal issues.
- 6.** The amount of time the potential target spends online.
- 7.** The type of information the potential target posts or shares on their social networking profiles (i.e. Facebook, MySpace, MyYearbook, LinkedIn, etc.).
- 8.** The potential target's offline demeanor leading the iPredator to conclude the online user will be an easy target.
- 9.** The non-response or lack of assertive confrontation by a potential target to respond to negative information.
- 10.** The potential target's probability of not having social system support, legal/law enforcement support or knowledge of intervention strategies if cyber attacked.
- 11.** The quantity and themes of images and/or videos an online user posts or shares online.
- 12.** The pattern of "*likes*" and "*dislikes*" an online user posts or shares on their social networking profiles.
- 13.** The frequency a potential target changes their profile images and information on their social networking profiles.
- 14.** Images and/or videos showing the potential target's economic status, the layout of their residence or their material objects they or their loved ones own.
- 15.** Images, videos and posts of the potential targets choice of lifestyle and/or material objects.
- 16.** Images, videos and posts of the potential targets lifestyle.
- 17.** Images, videos and posts of the potential targets needs, wants and desires.
- 18.** Images, videos and posts suggesting the potential target is suffering from psychological and/or psychosocial dysfunction.

Although there are other factors an iPredator uses in their repertoire of exhibiting IVI, the eighteen factors listed are recommended to evaluate by all online users to reduce their chances of becoming an iPredator target. Not included in these factors and apply to all online users is the unfortunate reality of being targeted by an iPredator as part of a mass trolling scheme. This occurs most often in cyber crime when the potential target receives an email asking them to open an attachment or gulled into providing personal information. This cyber crime and cyber bullying tactic is called "*Phishing*."

An iPredator's IVI acumen is based on practice, trial and error, understanding of human behavior and knowledge of Internet safety practices and Information and Communications Technology. Just as a locksmith has expertise at unlocking locks,



an iPredator has expertise choosing a target they have concluded will not cause them to be identified, apprehended or punished. An iPredator's IVI falls upon a continuum of dexterity whereby some iPredators are advanced in their IVI skills and other iPredators are novices. Whether the iPredator is advanced or novice in their IVI acumen, the fact that they engage in developing an IVI makes them a potentially dangerous online user.

In addition to having IVI, the iPredator practices Cyberstealth using multiple covert strategies. In fact, the third criteria used to define an iPredator include a general understanding of Cyberstealth used to profile, identify, locate, stalk and engage a target. Also lying upon a continuum of expertise, iPredators are assessed as being advanced in their Cyberstealth practices as opposed to a haphazard approach of targeting a victim without attempting to hide their identity. Often times, cyber bullies, ex-partners, ex-employees, angry or self righteous online users, Internet trolls, organized groups with political, religious, moralistic causes, [child molesters](#), [pedophiles](#) and highly narcissistic online users do not attempt to hide their identities. Cyberstealth is a strategy reserved for iPredators who seek to hide their true identities online.

Cyberstealth, a concept formulated along with iPredator, is a term used to define a method and/or strategies by which iPredators devise tactics to establish and sustain complete anonymity while they troll and stalk an online target. In addition to a stratagem, Cyberstealth is a reality of Information and Communications Technology, that humanity often fails to fathom leading some online users to become high probability targets. Cyberstealth is a learned behavior that becomes more advanced with practice, trial and error and experimentation.

For some iPredators, they seek the advice and consultation of other iPredators to hone their skills. In the realm of hacking, some iPredators actively seek the insight from other hackers to advance their knowledge base. Although "hackers" tend to be considered by the general mainstream as nefarious, there are two distinct groups defined by their motivations. "[Black Hat Hackers](#)" engage in nefarious and malevolent online activities. "[White Hat Hackers](#)" are Information and Communications Technology security experts.

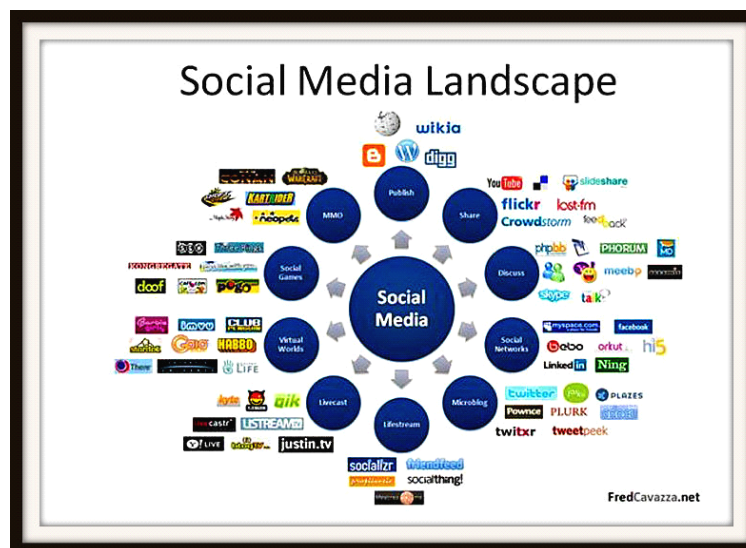
Given the Internet inherently affords everyone's anonymity, Cyberstealth used by iPredators range from negligible to highly complex and multi-faceted. Like IVI, Cyberstealth is a learned behavior that becomes more advanced through trial and error, experimentation, consultation with other online users who engage in malevolent or nefarious activities and investigation of Information and Communications Technology products and services focused on hiding an online user's identity and the ability to engage in anonymous surveillance. In addition to being a learned behavior, Cyberstealth may also include an inherited aptitude, capacity or skill set just as some people have special skills for certain things even though they are new to a craft.

The rationale for using "[stealth](#)" in the suffix of Cyberstealth, serves to remind online users the primary intent fueling many iPredators. This motivation is to hide their identity by designing fictive online profiles; identities, tactics and methods to ensure their identities remain concealed reducing recognition and castigation. Therefore, as the Internet naturally offers all online users' anonymity if they decide, iPredators actively design online profiles and diversionary tactics to remain undetected and untraceable.

**Stealth:** According to the Merriam-Webster dictionary, Stealth is "*the act or action of proceeding furtively, secretly, or imperceptibly.*" Stealth as an adjective is, "*intended not to attract attention.*" The American Heritage dictionary defines Stealth as "*the act of moving, proceeding or acting in a covert way and the quality or characteristic of being furtive or covert.*"

Cyberstealth is a covert method by which iPredators are able to establish and sustain complete anonymity while they engage in online activities planning their next assault, investigating innovative surveillance technologies or researching the social profiles of their next target. When profiling or conducting an investigation of an iPredator, the level of Cyberstealth complexity and online footprint for identification and apprehension are used.

As stated above, iPredator is a global concept that includes children, adults and organized groups who use Information and Communications Technology to harm other innocent, vulnerable and unsuspecting online users. The goal of the United States is to stop the growth of iPredator by educating its citizens on their tactics and strategies. From a profiling and investigation standpoint, assessment of an iPredator's Cyberstealth tactics and [Digital Footprint](#) can assist authorities in their profiling, identification and apprehension. Just as classic criminal profiles have [signatures](#) used to apprehend them, iPredators have digital signatures as well.

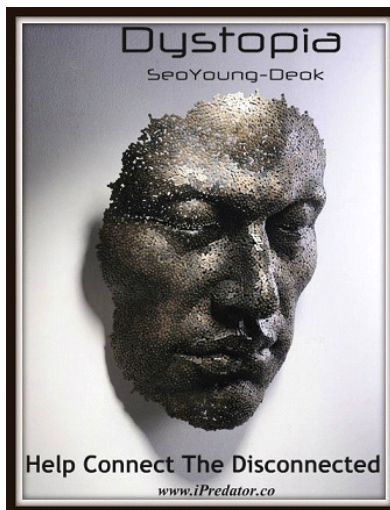


Technological advancements have changed the way humanity interacts, exchanges and accesses information. Smartphones, mobile devices and social media are the latest in a succession of advancements growing at a feverish pace. It is often difficult to imagine that the Internet used by two billion plus people globally celebrated its 20th birthday in 2011. Clearly, the [Information Age](#) has spread to all corners of the planet.

As of December 31, 2011, [Nielsen Online](#), [International Telecommunications Union](#), [GfK](#) and [Internet World Stats](#) estimate 2,267,233,742 people globally are Internet users having grown by 528% from 2000-2011. Despite its already significant impact, the pace of new-technology introductions and number of Internet users will continue to grow at an accelerated rate with access to and the exchange of information being a priori. The [Cisco Visual Networking Index 2010-2015 Forecast](#) predicts that the number of global Internet users will reach 3 billion people, 40% of the world's population, by 2015. Even more astonishing, by 2015, 1,000,000 minutes of video per second will stream over the Internet.

Although Information and Communications Technology benefits far outweigh detriments for society, humanity has been seduced by the notion that more technology translates into a better quality of life. Along with this distorted societal perception, humanity also fails to heed the warnings of prophetic authors of the past century that wrote about chilling glimpses of a [Dystopia](#) society. A Dystopia in literature portrays a society on the edge of destruction and authoritarian control.

Personal freedoms banished from society, leaving citizens at the mercy of the government's eccentric rules and demands. As seen at the individual level, the effects would be devastating and shocking. In such an atmosphere, citizens would become demoralized, conditioned in thoughts and actions to adhere to administrative goals, experience a loss of independence and forfeiture of self-reliance due to the constraints by governments placed on free will.



Dystopia is "*the concept of humans abusing technology and humans individually and collectively coping, or not being able to properly cope with technology that has progressed far more rapidly than humanity's spiritual evolution. Dystopia societies are often imagined as police states, with unlimited power over the citizens.*" ([Wikipedia](#))

Nowhere is the picture of Dystopia more clearly depicted than through the literary genre of science fiction. Expressed in the literary works of writers such as [Ray Bradbury](#), [Aldous Huxley](#) and [George Orwell](#), humanity becomes increasingly separate from one another led by technology. If not addressed, some predict humanity will enter an age that is the embodiment of Dystopia depicted in Ray Bradbury's novel, "[Fahrenheit 451](#)." The similarities between humanity's current condition and Ray Bradbury's well-crafted, cold, detached characters in Fahrenheit 451 are intriguing to say the least. Bradbury's depiction of a society in which technology has replaced human effort and thought, eerily parallels technological forecasts of contemporary culture.

***"We are living in a time when flowers are trying to live on flowers, instead of growing on good rain and black loam." – Faber (Fahrenheit 451.)***

The concept of being "connected" paradoxically makes us less connected to what is really happening globally. As Information and Communications Technology becomes increasingly widespread, the less we know our neighbors and the more we assume we know the people with whom we are "connected" to online. Humanity slowly separates, isolates and disconnects from human contact on a real human and spiritual level.

Society is being lulled into a false sense of trust and reliance on technology, taking information and "connection" to others in cyberspace at face value. Like the child in the fairy tale, [Little Red Riding Hood](#), innocently wandering through the forest, we erroneously believe that the "Wolf" is whoever he appears or claims to be. Just as Little Red Riding Hood, we are in danger of falling prey to a predator called iPredator.

Although disguised, Little Red Riding could see her predator, whereas we cannot thanks to Cyberstealth and the inherent anonymity provided by Information and Communications Technology. It is amazing how this fairy tale, created centuries ago, evolved to become a story about a child that resembles the tactics of impersonation used in cyber bullying and online sexual predator stalking and "grooming." Unfortunately, the theme of an iPredator disguised, as someone else is exactly what now occurs in [cyberspace](#).

By virtue of this proverbial "cloak of anonymity" so conveniently provided by Information and Communications Technology, iPredators troll cyberspace with a distinct advantage in their ability to represent themselves in any way they choose. Furthermore, they can secretly stalk their prey by tracking the potential

victim's path from an undetectable, safe distance. Not only can iPredators become anyone they choose to be, they can also become anyone their victim may subconsciously desire them to be.

The repercussions of the unrestricted latitude of iPredators will be catastrophic for not only the individual, but for society, and potentially, the world over. Therefore, before it is too late, society must re-examine the phenomenon of "[social networking](#)" via technology. Humanity must become educated in the [Dark Psychology](#) of Information and Communications Technology and learn to respect the mighty potential for harm that lurks beneath its surface. Society has now become ripe for the birth and growth of a new human predator advanced in all things Internet. This deviant's name is an iPredator.

The arena iPredators stalk their targets is cyberspace with physical contact often a secondary objective. Cyberspace is a hypothetical environment involving all online users interconnected through computers, telecommunications and the Internet without regard to physical location. [William Gibson](#) invented the term cyberspace, which he used in his 1984 novel, [Neuromancer](#).

In 2012, cyberspace describes the non-physical terrain created by Information and Communications Technology. In its advanced form, cyberspace has evolved into [virtual reality](#). Online users presented with visual, auditory and tactile feedback experience virtual reality in cyberspace as a real domain. Thus, virtual reality creates a perceptual illusion mimicking a realistic atmosphere. As virtual reality progresses in its endeavor to mimic physical reality, humanity continues to be amazed by the perceptual reality created, even though virtual reality is a mere infant in its inevitable development.

Whereas virtual reality is positive and artificial, iPredators are both very real and potentially very dangerous. In all cases, iPredators exhibit minimal disquiet for the victim's psychological welfare by injecting fear, embarrassment and distress in their lives. As stated, the iPredator is the antithesis to the positive environment created by virtual reality. It is also fair to assume that iPredators will include virtual reality in their future Cyberstealth strategies as technology advances. Given virtual reality is an illusion, why would iPredators not incorporate this growing technology into their criminal, deviant or abusive strategies? The goal is not to be one step ahead of iPredators, but know they exist.

Unlike traditional human predators prior to the [Information Age](#), iPredators rely on the multitude of benefits offered by Information and Communications Technology. These assistances include exchange of information over long distances, rapidity of information exchanged and the seemingly infinite access to the data available. Malevolent in intent, iPredators rely on their capacity to deceive others using Information and Communications Technology in an abstract electronic universe. Within the next three decades, iPredator acts of theft,



violence, abuse, [cyber warfare](#) and [cyber terrorism](#) will grow into a global plague if not quashed and thwarted. Society cannot rely on governments to confront all groups of iPredators because iPredators are everywhere and live within our communities.

In early 2011, United States intelligence officials raised concerns about the growing vulnerability the United States faced with cyber warfare threats and malicious computer activity. [C.I.A.](#) Director, Leon Panetta testified on Capitol Hill before the [House Permanent Select Committee](#) on Intelligence stating, "*The potential for the next Pearl Harbor could very well be a cyber-attack.*" The [Director of National Intelligence](#), James Clapper testified stating, "*This threat is increasing in scope and scale, and its impact is difficult to overstate.*" Clapper also stated, "*There are roughly 60,000 new malicious computer programs identified each day.*" "*Some of these are what we define as advanced, persistent threats, which are difficult to detect and counter.*" Director Panetta also stated to the committee, "*This is a real national security threat that we have to pay attention to. I know there are a lot of aspects to it. The Internet, the cyber-arena ... is a vastly growing area of information that can be used and abused in a number of ways.*"



As of 2012, United States officials from the [National Security Agency](#), [Department of Homeland Security](#) and the [F.B.I.](#) continue to prepare for cyber security threats. The military activated the [United States Cyber Command](#) in 2009 to coordinate the military's cyberspace resources. The United States Cyber Command functions to counter national security threats to the Pentagon's information networks and the United States cyberspace operations and intelligence. As the United States and the rest of the world's industrialized nations prepare for cyber warfare and cyber terrorism, the global community must also concurrently prepare for both cyber terrorism and homeland iPredators.

As described, iPredators use a tactical weapon I have termed "Cyberstealth" furnished by Information and Communications Technology. Cyberstealth is a



method iPredators create and implement while they taunt, troll and stalk their prey. iPredators target online users, corporate entities and organized groups oblivious, inexperienced, ill informed or unaware they are covertly being evaluated as a potential target for a cyber attack.

In nature, wild animals stalk and measure their prey using stealth and tactical strategies increasing their probability of success while decreasing potential for injury. iPredators also use stealth, Cyberstealth, to stalk online users increasing the probability of achieving their aims, while decreasing their potential of identification and punishment. As I illustrate in my theoretical report, [Dark Psychology](#), humans are the only living organisms that stalk, hunt and attack their own species without the primary instinctual drives of procreation, territorial control, survival or food. Although humanity is the apex living organism on Earth, we are also the apex of brutality upon ourselves and other living creatures.

The prime targets sought by iPredators are online users not intellectually, psychologically and technologically equipped. Their targets lack Information and Communications Technology safety strategies and technology, heightened levels of awareness online, a healthy level of skepticism, comprehensive digital citizenship practices and [C3 \(cyber safety, cyber security and cyber ethics\)](#) plans.

Using Cyberstealth, iPredators have considerably lower probabilities of identification, legal ramifications or injury. Prior to Information and Communications Technology, assailants had to be far more creative in their methods. Now equipped with Information and Communications Technology and trained in Cyberstealth, they can create counterfeit identities or manipulate others using embellished personas of who they envision themselves to be most influential to others. If they so choose, iPredators can start and end their day sitting in their home in front of their computer [ad infinitum](#).

Computer science experts, sociologists and psychologists tend to describe Information and Communications Technology and the Internet as beneficial tools for humanity. Based on my investigative findings leading to the creation of iPredator, I perceive this new dimension and the tools required for access quite differently. Although I regard the [World Wide Web](#), [Telecommunications](#), [Digital Technology](#) and [Mobile Device Technology](#) as all highly beneficial tools and areas extremely helpful to society, I do recognize tools have many different purposes. When chosen for nefarious or malevolent reasons, Information and Communications Technology and the Internet are tools that become weapons. iPredators primarily use Information and Communications Technology and the Internet as weapons in their efforts to offend, dominate, control or steal.

Unlike any other tool, Information and Communications Technology and the Internet, as weapons, can cause horrible and deadly consequences to both the citizens and communities of the countries they hail from. The future of [Cyber Warfare](#) and [Cyber Terrorism](#) are both inevitable realities that have yet, in 2012,

cause massive harm to society. As this writer continues to research the growth, expansion and underpinnings of iPredators, he has concluded Cyber Warfare and Cyber Terrorism will become terms feared by humanity within the next two decades. Within five decades, most industrialized nations will allocate a majority of their defense budgets to protecting their citizens from the potential devastation caused by iPredators.

Prior to Information and Communications Technology, all methods of communication involved some form of identification and response recognition skills using at least one of the five senses. Although deception, crime and immoral acts were committed, they entailed far more creativity, design and planning than what is required online and in cyber space. Even when tribes used smoke signals to communicate hundreds of years ago, the group watching the signals had a rough estimate of who were the senders and what location the messages were coming from.

In cyberspace, our physical senses are relatively subdued as we exchange and/or verify information. Online users attempt to identify and validate information as valid, at times, completely isolated from the source. The "*veil of invisibility*" that Information and Communications Technology and cyberspace offers humanity has numerous benefits, but the detriments can far outweigh the assistances for the vulnerable, unaware or ignorant online user.

iPredators use Cyberstealth for vindictive, abusive, malevolent or criminal pursuits. They purposely strategize and plan how they will use Cyberstealth without the negative consequences of law enforcement or authority figure identification. The energy required in planning and designing Cyberstealth strategies by an iPredator correlates with their perverse objectives. To the child cyber bully, they tend to practice minimal online deception given they are fueled by needs of recognition and peer acceptance. Depending on the cyber bullies strategy of taunting and harassment, their Cyberstealth may range from non-existent to cyber bullying by proxy.

[Cyber bullying by proxy](#) is when a cyber bully coerces or encourages other online users, who do not know the target victim, to become an accomplice of the cyber bully and join in assaulting, taunting or harassing the target child. The unfortunate reality for the target child is they are deluged by hurtful and harassing information not necessarily knowing who or how many online users are attacking them. Cyber bullying by proxy and truly a heinous act committed upon children.

At the advanced end of the Cyberstealth continuum are online sexual predators, cyber criminals and those seeking to target online users motivated by violent and/or sadistic intent. Although the majority of child sexual assaults takes place offline by friends, family members and young adults close in age to the target child, there still are thousands of online sexual predators, confirmed by the FBI,

trolling online for discouraged, easily manipulated children. In May 2011, the FBI released a short video to the public reporting there were 750,000 child predators online at any given time. Although this number is astronomical, this writer does not recall this unfortunate and alarming estimate being reported on the nightly news or in the headlines in print media.



As part of the human condition, we tend to embellish our attributes, both offline & online endeavoring to present ourselves as more successful, popular, rich, attractive and worldly. The purpose of embellishing our attributes is not to abuse or victimize the recipient, but to increase our perceived worth. This form of "bragging" or embellishing" has been social aspects of interpersonal relationships since the beginning of humanity. Presenting ourselves in the best possible light is not only restricted to humans, but occurs among the vast majority of living organisms as well. A male Peacock does not unfurl his massive blue plumes of feathers simply to air them out; he does this to show other Peacocks he is healthy and valuable. In cyberspace, online users who brag about their attributes or material wealth are practicing the same deceptive behavior as the Peacock.

When used for malevolent or nefarious purposes online, this innate capacity we all have to bolster our image becomes part of Cyberstealth used by iPredators. If an online user is caught engaging in felonious statements about themselves, but they do not meet the three criteria for defining iPredator, then their online exaggerations and deceptions do not fit into the definition of Cyberstealth. Online deception requires the motivation to harm other online users in order to meet criteria for iPredator.

Although being the online recipient of bogus information about another online user can be both frustrating and laughable, it does not suggest they are an iPredator. Cyberstealth are methods used by an iPredator and a tactic with intent to harm as opposed to impress. Information and Communications Technology and the Internet can paralyze our innate evolved instincts for "[survival of the fittest](#)" and cause us to lose sight of being skeptical and wary of people we meet online. For this reason, it is always vital to be wary about what others disclose online and the modus operandi behind their statements.

Although federal, state, and local officials work diligently to combat iPredators, their endeavors, as of 2012, are minimal at best given the size of the iPredator contingent. iPredators have the luxury of trolling for victims at a leisurely pace without fear of punishment. Unassuming online users are easily lulled into complacency and let the digital defenses down because they are either ignorant to iPredator Cyberstealth practices, seeking social acceptance by someone they think will "like them" or engaged in high-risk online behaviors increasing their probability of being targeted. The reasons for online users engaging in high-risk behaviors are multi-faceted, but relied upon by iPredators in order for their Cyberstealth to be effective.

Cyberstealth is an iPredators most powerful weapon in their strategy hunting online human quarry. In order for an iPredator's Cyberstealth strategy to be successful, they must affiliate and/or target online users who are distracted, distressed, discouraged or dysfunctional (D4). The symbol, D4, is used as a mnemonic device to encourage all online users to maintain awareness of their psychological functioning when interacting with others online. What minimal research to date has concluded on psychological functioning and online victimization is that an online user's mental state will hinder their ability to practice responsible and safe Information and Communications Technology activities.

Fueled by [anger](#), [depression](#), [greed](#), [narcissism](#) and/or [sociopathy](#), many iPredators revel in their Information and Communications Technology anonymity. Many also become grandiose from their criminal and abusive triumphs and feel galvanized knowing they can freely troll for potential victims, seemingly immune from law enforcement identification or apprehension. Depending on their relationship to the victim, iPredators have the freedom to preserve or divulge their identity at will.

Without fearing reprimand, iPredators participate in creative design and focused purpose in their line of attack. As part of the human condition, all humans experience exhilaration and/or satisfaction when they are triumphant. For iPredators, they experience the same states of exuberance, but at the expense of their victim(s). The more malevolent the iPredators' endeavors are, the greater sense of accomplishment they feel as they prevail.

Within the next 5 years, [smartphones](#) will surpass personal computers for connecting to the Internet. By the end of 2012, the number of mobile connected devices will exceed the world's population and by 2016, there will be over 10 billion mobile-connected devices, including machine-to-machine (M2M) modules that will exceed the world's population of 7.3 billion people ([Cisco VNI Forecast.](#)) Given the obvious benefits Information and Communications Technology offers, time spent interacting online will increasingly become commonplace for all humanity.

The new dimension of cyberspace is uncharted territory filled with opportunity and hope. The antitheses to these opportunities are iPredators. Without strict penal regulations, a sustained law enforcement presence and structured educational methods, cyberspace will become a prime hunting environment for iPredators' abusive, criminal or sexually deviant pursuits.

Although this writer staunchly advocates for online privacy, iPredators must have ingrained in the back of their minds a serious potential exists for their identification, apprehension and prosecution when they engage in nefarious and/or malevolent online activities. The future of mobile is now upon humanity, but only the Information and Communications Technology forecasters and criminal science experts understand the dangers to online users if not prepared. As of 2012, Internet security experts report mobile device technology continues to grow, but network security and cyber security remain too simplistic. A world with each and every citizen walking around with unsecured mobile devices is "iPredator Utopia."

***"Mobile media communication has turned the world into a global information hub." (MOCOM 2020, 2009.)***



## **5PV MODEL**

5PV is a five factor theoretic model used to conceptualize digital abuser/victim dynamics and all social interactions between people who use Information and Communications Technology and the Internet. These online users are segmented into three distinct groups categorized by their online intent, actions and motivations. The first group is online users who access and interact with other

online users for benevolent and/or purely social reasons. They use the Internet for what it was intended for and do not use cyberspace to offend, steal from or harm others. The opposite of this group are the iPredators who use Information and Communications Technology and the Internet to harm, victimize, steal from or abuse others.

Just as in humanity's offline environment, cyberspace has thieves, criminals, deviants and those who seek to harm others. Given there is no accurate way to validate the number of iPredators, this writer believes there are far more iPredators than there are offline criminals, deviants, bullies and assailants. The rationale for this assumption is based on the understanding of the anonymous environment provided in cyberspace available to all online users. When using a desktop computer or mobile device, there is not a person and/or authority figure standing before us monitoring and observing our actions. In cyberspace, the online user has complete privacy and anonymity.

Although privacy and anonymity can be enjoyable environmental states, those with villainous and/or secret enterprises use this anonymity to suit their selfish goals. For this reason, cyberspace is a perfect open territory for those who set out to abuse or victimize others. The group of online users that combine with the overt criminals, assailants and deviants are those who have always thought about or wanted to engage in asocial behaviors, but never did fearing identification and castigation.

Given the Internet affords everyone total anonymity if they choose, the online user with ill intent can explore and/or activate his/her darkest secrets. Hence, this writer posits there are far many more iPredators online than human predators offline because of the anonymous environment created by cyberspace. This population of online users falls in between the malevolent and benevolent groups and make up the third and largest percentage of online users. Just as offline humanity walks through life having their moral turpitude tested, online users experience the same tests regarding their intent, actions and motivations. The primary difference is these tests in cyberspace are not graded by authority figures and/or loved ones.

The five terms pertaining to the 5PV model of digital abuser/victim dynamics are iPredator, iPrey, iPrevention, iPreservation and iVictim. The 5PV Model is a representation of the five elements involved in all Information and Communications Technology, cyberspace and the criminal, deviant or abusive interactions between online users.

The primary difference between the 5PV model and other criminal and deviant victimization dynamics is the environment in which offender and victim interact. This environment, which benefits iPredator, is the [Geosocial Universe](#). Unlike any other territory, cyberspace is a frontier where the potential victim has little authority to evaluate their social exchanges in a realistic way.



Information and Communications Technology and Cyberstealth have afforded the criminal, deviant and sociopath pristine anonymity in their hunt for potential victims. It is in this realm, cyberspace, that iPredators are able to create a persona judged effective in their tactical strategy to achieve success in stalking. Without fear of identification, many iPredators have free reign to behave, interact and personify what they believe to be their most successful scheme. As social networking sites for all aspects of social functioning continue to expand, the territory for iPredators to locate and hunt their targets enlarges as well.

For example, a forty-year-old man can create an online social profile exactly how he feels will be viewed as most favorable by his target. If his prey is a 14-year-old female, he can download adolescent images, develop a creative teen background set up a felonious social profile and then interact with his teen targets as someone close to their age, same gender, stage in life and all the same "likes" and "dislikes" often discussed and rated online. Meanwhile, his potential targets innocently interact with him completely ignorant of his true identity. This is only one example of the hundreds of ways iPredators use Cyberstealth in cyberspace. Cyberspace and the online world provide iPredators a forum for pristine virtual reality and a forum to seduce their prey into believing their online identities are their true identities and/or their stated motivations are genuine and innocent.

Virtual reality is a term that applies to computer-simulated environments that can simulate the physical presence in places in the real world, as well as in imaginary worlds. Although virtual reality is a new science, this writer can guarantee some iPredators will follow its progression every step of the way. In cyberspace, iPredators no longer have to hide behind the proverbial bushes and they can skulk about in the dimension of cyberspace undetected, hidden and cloaked to perfection. Many iPredators evaluate their target quarry by first assessing if they are exercising personal security, harm reduction or victim prevention measures.

The concept that I have termed iPrevention, describes an online users sustained practice of Internet safety, cyber security and self-awareness of how they are perceived both offline and online. iPrevention is a strategy, practice and conscious sustained approach to reducing the probability of becoming an iVictim. These strategies involve a concerted effort to learn personal aspects and relevant demographic information about oneself that would increase the chances of becoming a target. If an iPredator resides near and/or is in close geographic proximity to their target, they will use theirs and informant observations to estimate the success rate of their cyber attack.

As Information and Communications Technology will always advance, iPrevention as well must be a proactive and progressive activity. This is not to say that iPrevention requires advanced training in Information and Communications Technology, but a sustained effort to learn and evolve given its rapid expansion. What is required is a willingness to exercise diligent awareness and confirmed

acceptance that some iPredators will always be one-step ahead in technological acumen.

Under the theory of iPrevention, the goal is not to be a step ahead of iPredators, but being keenly aware that they are always on the prowl and are using creative Cyberstealth methods to find and stalk their prey. Internet users can reduce the probability of becoming an iVictim, while accessing Information and Communications Technology, by practicing consistent & effective iPrevention. Just as everyone learns, practices and persistently work on developing their skills in any endeavor they strive to attain, the same methods apply to iPrevention. iPrevention is more than what not to post, share and how to behave online to prevent a cyber attack. iPrevention is also intervention strategies as well.

Equally important in iPrevention is what the online user does if and when they are cyber attacked. Given that the laws of probability state all online users will be confronted with some form of iPredator attack in their life, the steps one takes as soon as the cyber attack is initiated helps to reduce the negative consequences the attack intends to achieve. When instituting iPrevention, the online user is exhibiting iPreservation.

iPreservation is defined as an innate state of self-survival that manifests in an online user's Information and Communications Technology and cyberspace environment. Just as humanity has evolved their five senses to survive and thrive, humanity will now have to evolve a new sense to survive and thrive in the infant dimension of cyberspace. Using a symbolic equation, the importance of iPrevention & iPreservation to Internet safety is as follows:

## iPrevention = iPreservation

This simple equation represents a basic formula for all cyber protection and online safety initiatives by online users supporting humanity's constitutional survival instincts. Although cyberspace is clearly an abstract electronic universe that really does not exist, humanity both perceives and experiences the digital world as a genuine place having vital importance. iPreservation is an internal experience that signals the online user to behave and act accordingly when online or engaged in Information and Communications Technology usage.

Although self-preservation is ingrained in all living organisms, some online users lose this instinct in cyberspace. Just as the anonymity of cyberspace allows some online users to act and behave uncharacteristic of their true selves, the same phenomenon occurs in the realm of self-preservation. Because there is not another person and/or entity in front of them when online, some online users lose their natural proclivity to be cautious. iPreservation is both an innate instinct to survive and learned behavior to not want to be attacked. Even though an online user may be alone online, their iPreservation keeps them cautious in

the realm of cyberspace. iPreservation is the need and will to survive in the electronic universe called cyberspace.

In addition to the time spent and information shared while in cyberspace, advanced online safety skills also include an awareness of how offline behavior and lifestyle can modify online behavior. Far too many adults and parents of children fail to be cognizant that offline circumstances and psychological stressors dictate and govern online behaviors. In this writer's entire file of research and hours of investigation engaged in the formulation of the construct of iPredator, the one theme emphasized throughout its entire philosophical framework is as follows:

## Offline Distress Dictates Online Response (ODDOR)

Offline Distress Dictates Online Response or ODDOR posits that both a child and adult's response to their offline environment is directly correlated to how they behave online. When home, school, work, finances or other offline factors are causing significant distress, research has proven online users of all ages are more apt to be less vigilant in their Internet safety tactics and more likely to engage in high risk online behaviors. Under the concept of D4 (distracted, distressed, discouraged or dysfunctional,) online users that have been highly stressed offline are profiles the iPredator seeks to target. Depending on the advanced IVI (iPredator Victim Intuition) of the iPredator, an online users ODDOR can be quickly recognized by an iPredator.

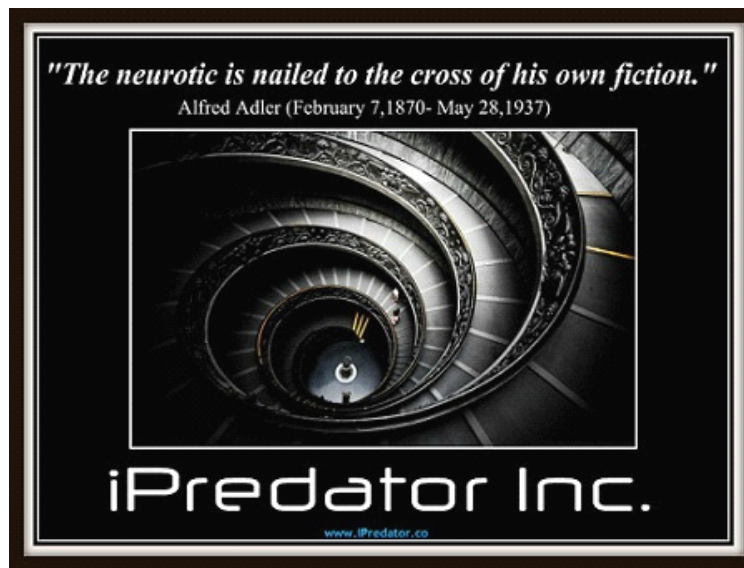
As stated, iPreservation is defined as an innate and learned reservoir of fuel or drive for lowering our probability of becoming a victim at the hands of an iPredator. This concept is an active "state of awareness" consistently observed by online users recognizing cyberspace is always an abstract concept and not a real dimension of space or reality. The innate need for survival should become pronounced in all of us in the digital world given that iPredators are protected by Cyberstealth, guided by conquest and domination and growing in numbers as Information and Communications Technology evolves and spreads.

iPreservation is also defined as an instinctual motivation to institute a set of behavioral goals in order to lower the probability of becoming a victim of an iPredator. iPreservation is both a state of being and a need to engage in the diligent practice of iPrevention. If someone is consciously aware that iPredators spend a considerable amount of time and energy trolling for vulnerable targets, that online user experiences a sense and/or need to preserve their safety and engage in the tactics and strategies to ensure their identity.

***"The motivation for iPreservation is not based on fear of iPredator, but rather, in the awareness they exist."  
Michael Nuccitelli Psy.D., C.F.C. (2012)***

The ideal target for an iPredator is an online user who does not take the necessary steps required to reduce their probability of becoming a [mark](#). High probability online user targets tend to practice denial, view themselves as too technologically advanced or outside the purview of an iPredator. When one or more of these elements are evident and/or perceived by online users, they are in the arena of an iPredator.

iPredator's antisocial pursuits are fueled by their distorted perceptions of self-preservation, narcissism and needs to dominate and control. For many of these miscreants, iPredators believe they must victimize others in order to thrive, sometimes to survive, to feel socially accepted and often for a sense of accomplishment, right or vindication. Their motivations to harm others are not always restrained by [guilt](#) or [remorse](#), because they perceive their actions towards a target and/or victim is deserved and the online user should have expected it given their attitude, actions or ignorance. Perceiving their actions in this way, iPredators justify the purpose of their malevolent and nefarious behaviors allowing them to harm others without feeling remorse.



Given that the concept of iPredator includes all online users, who attempt to taunt, victimize or abuse others using Information and Communications Technology, the easiest way to define the cornucopia of assailants and their core constructs are defined as lacking an Adlerian concept called, [Social Interest](#). Social Interest was postulated and defined by a turn of the century Austrian physician and psychologist, [Alfred Adler](#). In the simplest form, Social Interest, as defined by Alfred Adler, is an attitude or macroscopic outlook towards being charitable, helpful and interested in the personal pursuit of furthering the welfare of others. Adler went on to theorize that these elements of the human psyche, which inspired people to help others, are central to a person's sense of well-being, stable mental health and functional adaptability.

From this thesis, Adler strongly believed people with low Social Interest were discouraged, angry and enveloped by a sense of inferiority or by what he termed an [Inferiority Complex](#). Although Adler never experienced Information and Communications Technology and the advent of iPredators, his theory of Social Interest conceived almost a century ago certainly defines what appears to be an iPredator's proclivity to behave in an abusive, hostile, aggressive or criminal and deviant manner. As cost decreases with Information and Communications Technology, the population of Internet users will steadily increase.

Once again, iPredators use the same methodologies animal predators use in their hunt for food. The only difference being iPredators do not stalk for survival, food, procreation and/or territory. They stalk their quarry for deviant sexual needs, distorted sociopathic endeavors, criminal intentions, immature developmental needs to be accepted or psychological/psychiatric issues. iPredators tend to be male, but female iPredators are steadily growing at a rapid as Information and Communications Technology becomes more commonplace in daily living.

The entire population of online users in the 5PV model of criminal, deviant and harmful interaction between online users, called iPrey, represents all the potential targets in an iPredator's reservoir of possible choices. Everyone who interacts with Information and Communications Technology falls within this group. Just as a massive herd of [Wilbebeest](#) is all fair game to a pride of lions, so too are all online users potential targets to iPredators.

iPrey can be a low, medium or a high probability target for iPredators. Low probability targets are online users who are consciously aware there is malevolent people online who will attempt to victimize them if they let their guard down. Medium probability targets are as aware as low probability targets, yet are more susceptible given their age, gender or mental acumen. This is not to say that children, females or senior citizens cannot practice Internet safety or insulate themselves from victimization, but certain factors, age & gender, outside of their control, place them in preferred target populations of an iPredator.

High probability targets of iPrey are online users who do not practice online safety for various reasons. These reasons include ignorance to Internet safety and security, thinking they are irrelevant, simply not caring and/or knowingly engaging in high-risk online activities. Online users who are high probability targets are at an increased risk of becoming a member of the unfortunate group called iVictims.

The concept of iVictim, victimology and the development of victimization reduction strategies are all crucial to anyone who plans to be an active online user either for personal or professional use. Even when a person is a proactive online user, engaged in a healthy offline lifestyle, skilled at practicing Internet safety and diligent in their practices, it is still very important to regularly

investigate the field of victimology. The understanding of the 5PV Model and its philosophical underpinnings are extraordinarily important for children, adults and parents. iPredators seek out and stalk online users evaluated to be lax in practicing iPrevention while traveling through cyberspace. Everyone using Information and Communications Technology is a potential iVictim of an iPredator.

Just as wild animals and insects stalk their prey for food, iPredators seek online users they have deemed approachable. In the wild, predators stalk and hunt prey they have evaluated to be a highly favorable target, profiled to be the weakest and least intimidating. The most vulnerable targets for both the animal and insect predator and iPredators are the young, the old, the feeble or wounded. Given that the vast majority of iPredators tend to be males, they often target females due to their distorted perception that females are weaker and/or less clever.

This rule does not apply to cyber bullies, as these segments of iPredators are primarily same gender. The role of males being the predominant online assailants is quickly changing as Information and Communications Technology becomes more relevant to societal communications. Although in 2012 gender male continues to be the largest group of online offender, the rate of female iPredators steadily increases.

Ignorance, discouragement, psychologically compromised, lack of skepticism, isolative tendencies and curiosity are but a few traits an iPredator looks for in hunting for an iVictim. In addition to being adept at practicing Cyberstealth, iPredators are trained at sensing the qualities that they deem advantageous to initiate the hunt. By utilizing iPrevention tactics, an individual reduces their potential to becoming an iVictim while interfacing with Information and Communications Technology.



## **IPREDATOR BEHAVIORAL CATEGORIES**

The concept of iPredator is a global concept and as of 2012 includes the typologies as follows: Cyber Bullies, Cyber Stalkers, Cyber Harassers, Cyber Criminals, Online Child Predators, Cyber Terrorists and anyone who uses Information and Communications Technology and the Internet to anger others or



engage in deviant behaviors. This writer is confident with the expansion of Information and Communications Technology and the growing influence the Information Age has upon humanity, there will be a plethora of new ways for criminals, deviants, terrorists and other factions of society to harm, victimize and assault other humans. Brief descriptions of iPredator behavioral categories are presented for review.

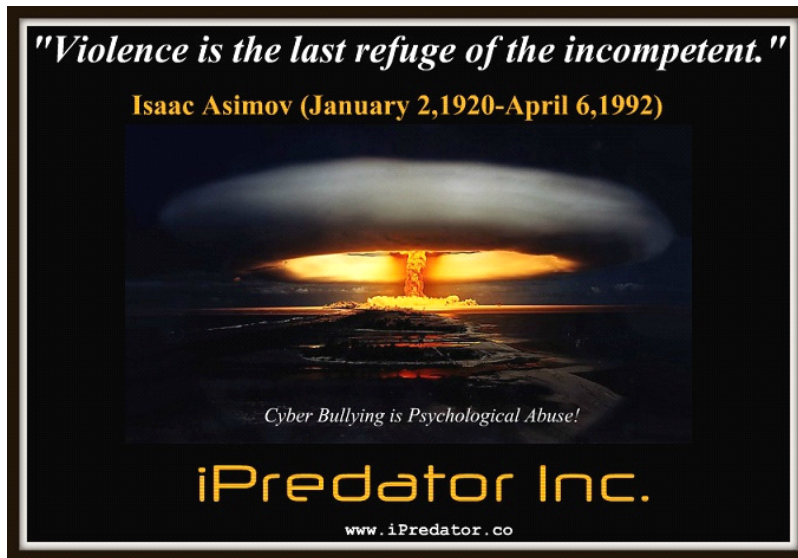
**Cyber Stalking:** Cyber stalking is defined as the use of Information and Communications Technology (ICT) to stalk, control, manipulate or habitually threaten a child, adult, business or group. Cyber stalking is both a tactic used by an ICT assailant and typology of pathological ICT user. Cyber stalking tactics include: false accusations, threats of harm, habitual monitoring, surveillance, implied threats, identity theft, damage to property and gathering information to manipulate and control their target. To meet the criteria of cyber stalking, the information and tactics used must involve a credible or implied physical and psychological threat to the target. An example of physical threat involves bodily harm to the target or their loved ones using ICT. Examples of psychological threats involve using disparagement, humiliation, disinformation dissemination and environmental damage to the target's reputation, credibility or financial status if the target does not acquiesce to the cyber stalker's demands.

**Cyber Harassment:** Cyber harassment is defined as the use of Information and Communications Technology (ICT) to harass, control, manipulate or habitually disparage a child, adult, business or group without a credible or implied threat of harm. Cyber harassment is a tactic used by an ICT assailant that may or may not be rooted in an attempt to control, dominate or manipulate their target. Although cyber harassment pertains to unrelenting taunting and disparaging information directed at a child, adult, public figure, group or business using ICT, the motivations of the assailant may be rooted in their own pathological drives and motivations devoid of the need to control, dominate or manipulate their target.

**Cyber Bullying:** Like classic bullying, cyber bullying is harmful, repeated and hostile behavior intended to taunt, deprecate & defame a targeted child. Cyber bullying describes threatening or disparaging information against a target child delivered through information and communications technology (ICT.) Unlike classic bullying, cyber bullying includes a phenomenon called Cyber Bullying by proxy. Cyber bullying by proxy is when a cyber bully encourages or persuades others to engage in deprecating and harassing a target child. Cyber bullying by proxy is a dangerous form of cyber bullying because adults may become the accomplices to the cyber bully involved in the harassment and do not know they are dealing with a child or someone they may know. A cyber bully is usually driven by a need for peer acceptance, but may engage in these maladaptive behaviors out of ignorance of the distress they cause a target child, or the most malevolent form, feels minimal remorse for the harm they are inflicting upon the target child.

**Cyber Crime:** Cyber crime is defined as crimes and criminal activity committed on the Internet using Information and Communications Technology as the tools to target victims. All forms of cyber crime involve both Information and Communications Technology and a targeted victim(s). Cyber crime is segmented into two distinct categories involving the focus of the cyber criminal activities. These activities are focalized on either the technology of Information and Communications Technology to achieve the cyber criminals aims for personal and/or financial gain or targeted at the person(s) using the Information and Communications Technology.

When the individual is the main target of cyber crime, Information and Communications Technology is the tool rather than the target. These are the crimes that have existed for centuries in offline society. Scams, theft, and fraud have existed long before the development of Information and Communications Technology. Cyber criminals utilize technological tools, which increases their potential pool of victims while making them difficult to identify and apprehend. Cyber crime targets people, property or governments.



**Cyber Terrorism:** Cyber terrorism is defined as the use of Information and Communications Technology (ICT) by iPredators, organized groups and/or terrorist groups to advance their agenda motivated by religious, political and/or philosophical ideologies. Examples of cyber terrorism include: 1. The use of ICT to organize and execute attacks against networks, and information and communications technology (ICT) infrastructures. 2. The exchanging of information or making threats electronically. 3. The act of hacking into computer systems. 4. Introducing viruses and malware to vulnerable networks. 5. Defacement of websites and blogs. 6. Denial-of-service attacks 7. Terrorist threats made via electronic communication.

When strategic cyber attacks are motivated for financial gain, these attacks are defined as cyber crime. Cyber terrorism is any premeditated, political, religious or philosophical motivated attack against information, computer systems, computer programs and data, which results in violence against non-combatant targets by sub-national groups or clandestine agents. A cyber terrorist attack is designed to cause physical violence or extreme financial harm to targeted victims or a community. According to the U.S. Commission on Critical Infrastructure Protection, cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.

The F.B.I. defines cyber terrorism as "*The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents.*"

**Online Predators:** The typology of iPredator that is categorized in Online Predators has a variety of different terms used to describe essentially the same patterns of abuse and motivations for the abuse. Online Predators are defined as adult online users who seek to exploit vulnerable children and/or adolescents for [sexual](#) or other abusive purposes. Online Predators are sexual predators who use Information and Communications technology and the Internet to locate, target and victimize minors. Common online forums used by Online Predators to target children include: chat rooms, instant messaging or social networking sites for the purpose of flirting with and meeting others for illicit sexual experiences.

Online Predators often manipulate or "groom" a minor with the ultimate goal of meeting and engaging in sexual activity, despite knowing they are engaging in illegal activities. In instances where meeting their victims to engage in sexual activities is not the primary objective, Online Predators also attempt to persuade children and adolescents to participate in some form of online sexual and/or sexually provocative activity. When online predators engage in this activity, they are motivated by sexual deviance and/or for financial gain on the distribution and sale of child pornography.



# INTERNET SAFETY FACTORS

In order to effectively educate, evaluate, investigate or advise any Information and Communications Technology (ICT) user on Internet safety, whether they are a child, adult, group or business, it is paramount to grasp the basic concepts and terms vital to all ICT users. The importance of ICT and the Internet to humanity is different to everyone and as unique as a fingerprint. For some, ICT and the Internet are nothing more than tools of convenience for conducting mundane tasks. For others, their social, scholastic, business and/or financial affairs disclosed online are crucial to their life functioning, self-esteem, self-worth, success and perceptual world.

***“In an abstract way, ICT and the Internet are extensions of the human mind, but made available to all who engage in benevolent & malevolent activities.” Michael Nuccitelli Psy.D., C.F.C., (2012)***

As ICT, social media, virtual reality and the information age rapidly expands becoming more integral to humanities daily activities, understanding the basic tenets of these new dimensions are preponderant. In 2011, the Internet celebrated its 20<sup>th</sup> birthday. In 2012, most of humanity continues to fail in understanding the golden rule of all new territory exploration. What always comes with opportunity and new frontiers are elements unknown and potentially dangerous. It is these unknown and dangerous elements lurking within cyberspace that all ICT users and their loved ones must be vigilant about.

Development of the theoretical constructs of iPredator and ICT Psychology being pioneered by this writer and his colleagues took hundreds of hours to compile and aggregate. This writer and his colleagues are also firmly aware they have only scratched the surface of a new dimension a mere 20 years old called the Internet and a new cultural paradigm shift in the ways humans obtain, exchange and disseminate information. Even after this extensive research project led to the creation of these theoretical postulates, this writer was confronted with a plethora of ever growing questions and quandaries in the present and future importance and of ICT and cyberspace. This being said, it is clear that the information age is creating changes in all forms of communication.

Regarding the theory of iPredator and all products, services and trainings this writer has designed to date, the terms and concepts listed below were used in their creation. This writer strongly believes these 20 facets of ICT's interface with criminal, deviant, and abusive behaviors will be central themes for many years to come. Although ICT will continue to advance in both applications and purposes, the terms and themes presented below will always be integral to ICT safety and security practices. They are as follows:

**1. ICT:** Information and Communications Technology (ICT) is an umbrella term used to define any electronic or digital communication device or application used to obtain, exchange or disseminate information. ICT stresses the role of unified communications and the integration of telecommunications, which enable users to create, access, store, transmit, and manipulate information. ICT consists of all forms of telecommunication, information technology, broadcast media, audio and video processing, transmission and network based control and monitoring functions. Information and communications technology today usually means computer-based management of data or ideas, but will continue to grow with technological advancements. ICT has rapidly become one of the basic building blocks of modern society and will become increasingly important as the information age matures.

Many countries now regard understanding ICT and mastering the basic skills and concepts of ICT as part of the core of education, alongside reading, writing and mathematics. The importance of ICT to humanity lies upon a continuum of relevance ranging from minimal impact to vital requirement regarding an ICT user's day-to-day activities. For some, ICT and the Internet are nothing more than tools of convenience for conducting their responsibilities. For others, their social, scholastic, business and/or financial affairs disclosed online are crucial to their self-esteem, self-worth, success and perceptual world.

**2. iPredator:** A child, adult or group who engages in exploitation, abuse, victimization, stalking, theft or disparagement of others using information and communications technology (ICT.) iPredators are driven by deviant sexual fantasies, desires for power and control, retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance or personal and financial gain. iPredators can be any age, either gender and not bound by socioeconomic status or racial/national heritage. Whether the offender is a cyber bully, cyber stalker, cyber criminal, online sexual predator, Internet troll or cyber terrorist, they fall within the scope of iPredator. The three measures used to define an iPredator include:

**I. A Self-awareness of causing harm to others using ICT, II. Intermittent to frequent usage of ICT to obtain, exchange and disseminate harmful information and III. A general understanding of Cyberstealth used to locate, stalk and engage a target using ICT.**

Unlike traditional human predators prior to the information age, iPredators rely on the multitude of benefits offered by ICT. These assistances include exchange of information over long distances, rapidity of information exchanged and the seemingly infinite access to the data available. Malevolent in intent, iPredators rely on their capacity to deceive others using ICT in an abstract electronic universe.

**3. ICT Psychology:** Information and Communications Technology (ICT) Psychology is the study of cognitive, affective, behavioral and perceptual states in humans related to their interactions with ICT and cyberspace. ICT is an umbrella term used to define any electronic or digital communication device or application used to obtain, exchange or disseminate information. Cyberspace is an abstract concept used to describe the non-physical terrain created by ICT. Within this terrain, people obtain, exchange and disseminate information relevant to their needs, goals, developmental requirements and responsibilities. Although ICT defines the devices and applications used to obtain, exchange and disseminate information, ICT Psychology examines ICT in relationship to the human interactions that occur using ICT to interface with cyberspace.

ICT Psychology investigates the cognitive, affective, behavioral and perceptual motivations and drives directly employed using ICT to communicate with an abstract digital environment. ICT Psychology requires a person to interact with ICT as part of their pursuits and responsibilities and assumes these interactions act as a virtual extension of the human mind and social interactions. Just as the field of Psychology has sub fields of specialty, ICT Psychology also has variations in scope. Where as Cyber Psychology and Internet Psychology examines human behavior related to cyberspace, ICT Psychology includes ICT as well.

**4. Cyber Harassment:** Cyber harassment is defined as the use of information and communications technology (ICT) to harass, control, manipulate or habitually disparage a child, adult, business or group without a credible or implied threat of harm. Unlike physical harassment requiring physical contact, cyber harassment occurs in cyberspace using ICT and is verbal, emotional or social abuse of a person based on their race, gender, religion, socioeconomic status, physical attributes, sexual orientation or beliefs. Cyber harassment is a tactic used by an ICT assailant that may or may not be rooted in an attempt to control, dominate or manipulate their target.

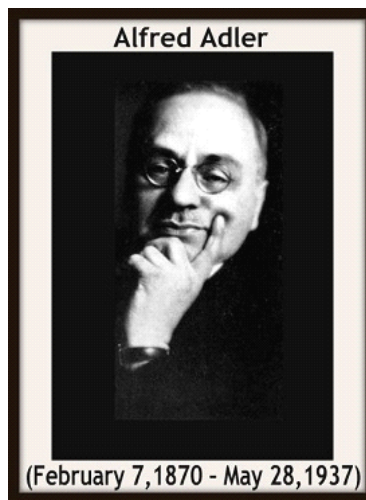
Although cyber harassment pertains to unrelenting taunting and disparaging information directed at a child, adult, public figure, group or business using ICT, the motivations of the assailant may be rooted in their own pathological drives and motivations. Cyber harassment differs from cyber stalking in that it is generally does not involve a credible or implied physical threat. Harassment does not include constitutionally protected activity or conduct that serves a legitimate purpose. In a rapidly expanding digital world, an ICT user's privacy and reputation becomes more vulnerable to corruption. As anonymity via the Internet becomes more feasible, cyber harassment continues to flourish. Cyber harassment is the adult form of cyber bullying to a minor.

**5. Cyber Stalking:** Cyber stalking is defined as the use of Information and Communications Technology (ICT) to stalk, control, manipulate, threaten or make unwanted advances towards a child, adult, business or group. Cyber stalking is both a tactic used by an ICT assailant and typology of pathological ICT



user. Cyber stalking tactics include: false accusations, threats of harm, habitual monitoring, surveillance, implied threats, identity theft, damage to property and gathering information to manipulate and control their target. To meet the criteria of cyber stalking, the information and tactics used must involve a credible or implied physical and psychological threat to the target. An example of physical threat involves bodily harm to the target or their loved ones via ICT.

Examples of psychological threats involve disparagement, humiliation, dis-information dissemination and environmental damage to the target's reputation, credibility or financial status if the target does not acquiesce to the cyber stalker's demands. The Internet is a global medium regardless of frontiers, and this creates new possibilities for the growing class of cyber stalkers. Given the Internet is inexpensive and easy to access, distance between cyber stalkers and their targets are no longer a confounding factor. Cyber stalking is both a strategy to target other ICT users and a psychiatric pathology. When Cyber stalking is a tactic, the assailant does not need to be motivated by psychiatric illness.



**6. Digital Reputation:** Digital Reputation is a term used to describe the reputation of an Information and Communications Technology (ICT) user or business that is disseminated online and available to peers, superiors, loved ones and consumers. This information can be positive or negative and vital to the health, success and reputation of an ICT user or the business. Digital Reputation is created and sustained by peers, school or work associates, loved ones, acquaintances, consumers, competitors, adversaries, online strangers and iPredators. Given the widespread growth and expansion of ICT, a positive digital reputation is vital to people, communities and business's in order to thrive, survive and the attainment of personal endeavors.

Digital Reputation and the growing risks confronting ICT users and businesses have become increasingly endemic due to the escalating use and significance of the Internet as a communication platform. With the ascent of social media, the

formation of Digital Reputation is an increasingly common process and the practices of Digital Reputation Management have become crucial for both individuals and corporate entities. An ICT user or business's Digital Reputation are directly correlated to their Digital Footprint. Like Digital Footprint, an ICT user's Digital Reputation is directly correlated to the quantity, quality, accuracy and extent of personal information they post or share online available and used by other ICT users.

**7. Digital Footprint:** Digital Footprint is a term used to describe the trail, traces or "footprints" that children, adults and businesses leave in cyberspace from their online activities using Information and Communications Technology (ICT.) This is information that is obtained, exchanged or disseminated between ICT users. An ICT user's Digital Footprint is created by social media information, forum registrations, e-mails, attachments, videos, digital images and other forms of communication via ICT that leave traces of personal and/or corporate information about someone and/or a business available to others online. An ICT user or business's Digital Reputation are directly correlated to their Digital Footprint.

An ICT user or business's Digital Reputation is created by a culmination of their Digital Footprints over a period of time. Like Digital Reputation, an ICT user's Digital Footprint can be positive or negative and vital to the health, success and reputation of an ICT user or the business. Personal information disclosed or shared online all contribute to an online user's Digital Footprint in the age of social media. Like Digital Footprint, an ICT user's Digital Reputation is directly correlated to the quantity, quality, accuracy and extent of personal information they post or share online available and used by other ICT users. It is for these reasons that a child, adult or business must be diligent in monitoring their Digital Footprint.

**8. High Risk ICT:** High Risk ICT factors are defined as actions and behaviors an Information and Communications Technology (ICT) user participates in online, which increases their probability of becoming a target of an iPredator. These actions and/or behaviors differ depending on the age, gender, environmental influences and psychological status of the online user interacting with ICT. High Risk ICT factors tend to be rooted in non-compliance, ignorance or oppositional defiance of following proper Internet safety and iPredator protection tactics when engaged in high-risk online behaviors.

High Risk ICT factors are highly susceptible to environmental stressors and psychological dysfunction. High Risk ICT factors tend to be most problematic for children, but adults can be equally susceptible. Of the myriad of high-risk behaviors an ICT user can engage in leading to an increased risk probability of being victimized, the following six behaviors are strong predictors of online victimization for children and correlated to adult online victimization:

**I.** Interacting online with unknown ICT users, **II.** Having unknown online users on their *"buddy"* or *"friends"* lists, **III.** Interacting online with unknown ICT users engaged in topics on sexuality, **IV.** Viewing or downloading pornographic or "dark" content online, **V.** Behaving in a rude, harassing or abusive manner towards other ICT users and **VI.** Posting or sharing personal and/or contact information available to unknown ICT users.

**9. ICT Awareness:** The ICT Awareness factor is defined as the level of awareness an Information and Communications Technology (ICT) user or business has related to their practice of Digital Citizenship and how other ICT users perceive them. This factor examines an ICT user or businesses' understanding of Digital Citizenship, cyber security and how other ICT users translate their ICT practices. ICT Awareness is a conscious state and overture that is part of a strategy, practice and consistent sustained approach to reducing the probability of being misrepresented by others or becoming an online victim. These strategies involve a concerted effort to understand how other ICT users perceive them. The ICT Awareness factor also describes the amount of information a parent, family member, support group, educator, loved one or business has accrued related to Digital Citizenship and Internet safety measures used to insulate a child, adult or business from becoming a target of an iPredator. The ICT Awareness factor includes:

**I.** The ICT user or business support system's understanding of ICT & Digital Citizenship, **II.** An iPredator's technique and tactics used in Cyberstealth with ICT, **III.** An ICT user's conscious effort to engage in Digital Citizenship and Internet safety habits and **IV.** An ICT user or businesses proactive self-monitoring of how other ICT users perceive them.

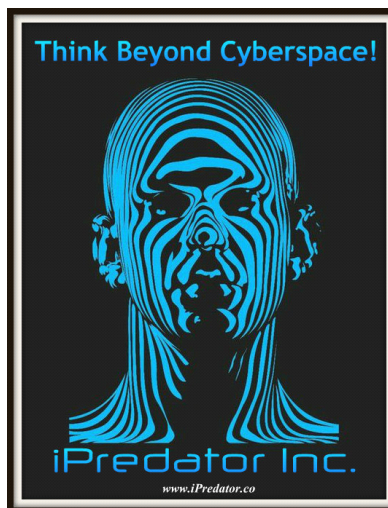
**10. Mobile Device Technology:** The Mobile Device Technology factor is defined as a collective term representing the portable genre of Information and Communications Technology (ICT) that describes the various types of mobile devices used by children, adults and businesses. Examples include cellular phones, smart phones and tablets. The Mobile Device Technology factor also relates to a child, adult or business's knowledge and application of mobile device safety. The term, Mobile Device, is a generic term used to refer to a variety of devices that allow people to access data and information from where ever they are. This includes cell phones, smartphones and various other portable devices.

The Mobile Device Technology factor also examines the child, adult or businesses' understanding of how they interact with their mobile devices and how iPredators use mobile device technology to target and locate their victims. However, mobility has far-reaching effects on the enterprise in areas such as security risk, use policies, manageability and governance. Given the rapid growth and inevitable broad expansion of mobile device technology, this area will become increasingly more relevant in regard to all ICT users practicing cautious and

proactive mobile device safety. Given the fast pace nature of human civilization, mobile device technology will become mandatory requirements for anyone seeking to connect with their loved ones, colleagues, peers and community resources.

**11. Personal Information:** The Personal Information factor is a term used to describe the quantity and frequency of personal information an Information and Communications Technology (ICT) user or business shares with other ICT users and available to known and unknown ICT users to view and prospect. Examples of personal information include: home/work/school address, full names, name of school/employer, age, gender, financial information, images, videos and online activities (i.e. passwords, usernames, profiles.) The Personal Information factor relates to the ICT user or business's knowledge and understanding of the risks created when they post and/or share their contact or personal information about their age, gender, daily routines, sexual predilections and online preferences and/or activities.

With an abundance of popular social networking websites like Facebook, MySpace, Twitter and LinkedIn, it has become easy for iPredators to target children and adults to amass their personal information. Images and videos posted publicly online can leave a trail easily traceable by iPredators. The Personal Information factor is the most important aspect of Internet safety cautioned to all ICT users. iPredators heavily rely on access and acquisition of their potential targets personal information. Given their advanced ICT prowess and ability to manipulate vulnerable ICT users, many iPredators do not have to rely on social networking sites to obtain the necessary personal information to locate, identify and target their victims.



**12. Psychological State:** The Psychological State factor is a generic term used to define psychological aspects of an Information and Communications Technology (ICT) user or group of ICT users at the time they engage in online activities and

how these psychological factors influence their capacity to practice Internet safety and security. The more isolated, discouraged or angry an ICT user feels, the more apt they are to engage in high-risk ICT activities discouraged by Internet safety guidelines. The Psychological State factor relates to the ICT user or business's knowledge and understanding of how cognitive, affective, behavioral and perceptual processing states govern ICT activities. Of the twenty factors designed in the iPredator theoretical construct, the ICT user's psychological state is primarily influenced by their home, career and/or school environments and highly relevant to their ICT activities and risk potential.

For all ICT users, their offline stressors, conflicts and environmental obstacles have a direct effect upon their ICT demeanor. And responses. When home, school, work, finances or other offline factors are causing significant distress, research has proven ICT users of all ages are more apt to be less vigilant in ICT and Internet safety tactics and more likely to engage in higher risk online behaviors. When an ICT user is in a perceived stable, encouraging, structured and consistent environment, their psychological well-being affords them to be more cautious and conscientious of their ICT activities.

**13. Social Media:** The Social Media factor is used to describe the online technologies and practices an Information and Communications Technology (ICT) user accesses to share their opinions, insights, experiences and perspectives related to their personal, career and/or scholastic activities on social networking websites. Social Media is defined as forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content. The Social Media factor relates to the ICT user's knowledge and understanding of their energy, time and importance they place on their social media profiles and networking endeavors, perceived online image and their interactions with other ICT users using social networking websites.

More specifically, Social Media refers to the use of web-based and mobile technologies to turn communication into an interactive dialogue. Within this factor, the areas investigated include the themes and quantity of personal and sensitive information an ICT user allows other ICT users to view related to themselves, their loved ones or their employers or academic institutions. A growing number of ICT users place an incredible amount of time, effort and thought into their social networking site profiles and endeavors. Social Media has become a driving force in many ICT users' lives and a frequented arena for cyber bullying, cyber harassment and cyber stalking.

**14. iPredator Protection:** The iPredator Protection factor is defined as the amount of effort, time and education an Information and Communications Technology (ICT) user or business engages in to reduce their probability of becoming a target of an iPredator. Slightly different than the ICT Awareness & iPredator Awareness factors used in the iPredator construct, iPredator Protection emphasizes the protective measures and protection based software, hardware

and applications an ICT user monitors, obtains and employs. The iPredator Protection factor relates to the ICT user or business's knowledge, participation and understanding of the necessary measures and strategies they should or should not engage in related to their ICT activities.

The iPredator Protection factor assesses if the ICT user or business actively practices ICT safety, cyber security, sets appropriate online restrictions and prepared to respond accordingly if they are targeted by an iPredator or nefarious corporate entity related to businesses. In relationship to children, the iPredator Protection factor also includes the effort, knowledge and tactics of parents, educators and the child's support system to insulate and protect them from iPredator. Just like any new environment humanity is presented, it is paramount for all ICT users to always be cautious when engaged in communications in cyberspace. ICT users adept at iPredator Protection are knowledgeable of all there is to protect themselves, their loved ones or business.

**15. iPredator Awareness:** The iPredator Awareness factor describes the amount of information, knowledge and conscious preparedness an Information and Communications Technology (ICT) user has related to iPredators and their existence in cyberspace. Vital to iPredator Awareness is an ICT user or business's capacity to understand the methods and techniques iPredators use to locate, identify, stalk and attack their target they deem as vulnerable and/or deserving of their victimization and stalking. The iPredator Awareness factor relates to the ICT users knowledge and understanding of the tactics and techniques an iPredator uses. iPredators can be any age, either gender and not bound by socioeconomic status or racial/national heritage.

Within each category of iPredator, a degree of victimization lies upon a continuum of severity ranging from mild to severe regarding their intent, goals and modus operandi. The key terms examines in the iPredator Awareness factor is awareness or a consistent level of caution practiced by the ICT user that is fueled by the ICT user or business's knowledge that iPredator's may launch a cyber attack. The level of iPredator Awareness practiced by an ICT user is defined by their psychological, emotional and environmental stability. The less stable the ICT user is with these human experiences, the less aware they are of the nefarious and malevolent entities that access ICT for vulnerable targets.

**16. Cyber Bullying:** Cyber bullying is defined as threatening or disparaging information directed at a target child delivered through information and communications technology (ICT.) Like classic bullying, cyber bullying is harmful, repeated and hostile behavior intended to taunt, embarrass, deprecate & defame a targeted child. Dissimilar to classic bullying, cyber bullying includes a phenomenon called Cyber Bullying by proxy. Cyber bullying by proxy is when a cyber bully encourages or persuades other ICT users to engage in deprecating and harassing a target child. Cyber bullying by proxy is a dangerous form of cyber bullying because adults may become accomplices to the cyber bully and may not



know they are dealing with a minor or child from their community. Cyber bullies are usually motivated by a need for peer acceptance and/or power and control.

A small percentage of cyber bullies engage in these maladaptive behaviors out of ignorance of the distress they cause a target child. The most malevolent form of cyber bully, feels minimal remorse for the harm they are inflicting upon the target child. It has been speculated that children view the real world and the online or virtual world as part of a seamless continuum. Unable to differentiate reality from virtual reality, victims of cyber bullying can become psychologically devastated and/or cyber bullies targeting children.

**17. ICT Forensic Psychology:** Information and Communications Technology (ICT) Forensic Psychology is a sub field of ICT Psychology and defined as the study of cognitive, affective, behavioral and perceptual states in humans related to their malevolent, nefarious, deviant or criminal interactions with ICT, cyberspace and their targets or victims. ICT is an umbrella term used to define any electronic or digital communication device or application used to obtain, exchange or disseminate information. Cyberspace is an abstract concept used to describe the non-physical terrain created by ICT. Within this terrain, people obtain, exchange and disseminate information relevant to their needs, goals, developmental requirements and responsibilities.

ICT Forensic Psychology explores the individual and group manifestations of behavioral, perceptual & psychological patterns within cyberspace in the areas of investigation and prevention of criminal violations, deviant behaviors and online victimization. ICT Forensic Psychology analyzes the psychological mechanisms by which antisocial views and habits arise and take root in a person or groups perceptual world, the process by which their criminal goals and motives are formed and how these criminal/deviant goals implemented involve ICT and cyberspace. ICT Forensic Psychology work to investigate and understand the psychological, behavioral and perceptual mechanisms of individuals and groups who utilize ICT to victimize, harm, cloak or steal from other ICT users, groups or businesses.

**18. Digital Citizenship:** Digital Citizenship is defined as the appropriate norms of behavior with regard to Information and Communications Technology (ICT) usage. Digital Citizenship addresses the multiple levels of responsibility encouraged for all ICT users when interacting with the devices & applications of ICT and cyberspace. The rules of Digital Citizenship include online etiquette, private information protection, online safety measures, dealing with cyber bullying and harassment, digital rights & responsibilities and cyber security. Digital Citizenship endeavors to advocate, model and teach others safe, legal, and ethical use of ICT including: respect for copyright, intellectual property and the appropriate documentation of sources. Educators of Digital Citizenship understand regional and global societal responsibilities in an evolving and rapidly expanding digital culture.

Although Digital Citizenship involves multiple facets, a primary goal is the practice of ICT etiquette and responsible social interactions. ICT etiquette are the electronic standards of conduct and behaviors when interacting with others and respect for the information one posts and disseminates regarding other ICT users. It is assumed the more skilled an ICT user is practicing Digital Citizenship, the less likely he/she is at being targeted by an iPredator. As described in the iPredator Protection factor used to create the theory of iPredator, Digital Citizenship is recognized as an iPredator Protection approach.

**19. Dark Psychology:** Dark Psychology is a theoretical construct designed by New York State licensed psychologist and certified forensic consultant. Dark Psychology is defined as the study of the human condition as it relates to the instinctual, sociological and psychological nature of people to prey upon others that falls along a continuum ranging from purposive and/or instinctual to purposeless and anti-evolutionary or evil. All of humanity has this potential to victimize other humans & living creatures. While many restrain or sublimate this tendency, some act upon these impulses. Dark Psychology seeks to understand the cognitive, affective, behavioral and perceptual states that lead to predatory behavior. Dark Psychology assumes that this production is purposive and has some rational, goal-oriented motivation 99% of the time. The remaining 1%, under Dark Psychology, is the brutal victimization of others without purposive intent or reasonably defined by evolutionary science or religious dogma.

Within the next century, the growth of Information and Communications Technology (ICT,) iPredators and their acts of theft, violence and abuse will become a global phenomenon and a societal epidemic if not squashed. Segments of iPredators include cyber stalkers, cyber bullies, cyber stalkers, cyber terrorists, cyber criminals, online sexual predators and political/religious fanatics engaged in cyber warfare. Just as Dark Psychology views all criminal/deviant behavior on a continuum of severity and purposive intent, the theory of iPredator follows the same framework, but involves abuse, theft, assault and victimization in cyberspace.

**20. Cyberstealth:** Cyberstealth, a concept formulated along with iPredator, is a term used to define a method and/or strategy by which iPredators use Information and Communications Technology (ICT), if they so choose, to establish and sustain complete anonymity while they troll and stalk a target. Given the Internet inherently affords everyone's anonymity, Cyberstealth used by iPredators range from negligible to highly complex and multi-faceted. The rationale for using "stealth" in the suffix of this term, serves to remind ICT users the primary intent fueling iPredators. This intent is to hide their identity by designing false online profiles, identities, covert tactics and methods to ensure their identities remain concealed reducing their probability of identification, apprehension and punishment.

Therefore, as the Internet naturally offers all ICT users' anonymity if they decide, iPredators actively design online profiles and diversionary tactics to remain undetected and untraceable. Cyberstealth is a covert method by which iPredators are able to establish and sustain complete anonymity while they engage in ICT activities planning their next assault, investigating innovative surveillance technologies or researching the social profiles of their next target. Concurrent with the concept of Cyberstealth is IVI or iPredator Victim Intuition. By using Cyberstealth, an iPredator's IVI is the aptitude to sense a target's online vulnerabilities, weaknesses and technological limitations increasing their success with minimal ramifications.

## 5PV MODEL NOTES

**5PV Model:** 5PV is a five factor theoretical model used to define all interactions between people who use Information and Communications Technology for personal and/or benevolent reasons and those who use Information and Communications Technology for selfish, nefarious and/or malevolent reasons. The five terms pertaining to 5PV are iPredator, iPrey, iPrevention, iPreservation and iVictim. The 5PV model is a representation of the five elements involved in criminal, deviant and abusive human interactions as they relate to the Internet and Information and Communications Technology. The primary difference between this model and all other criminal, deviant and abuse victimization models is the environment in which the interplay between predator and victim exchange occurs. This environment, which benefits iPredator, is cyberspace.

Unlike any other territory humanity has explored since the beginning of human civilization, cyberspace is a frontier where the potential iVictim has little grasp to evaluate social exchanges in a realistic way. For the first time in human history, the Internet has afforded human predators, iPredators, pristine anonymity. iPredators are able to create a persona they deem proper in their tactical strategy to achieve success in their methods of stalking. Without fear of identification, iPredators have free reign to behave, interact and personify what they believe to be their most successful strategy.

For example, a forty year old man can now create a profile to be exactly what he feels is most plausible to his target. If his prey is a fourteen year old female, he can download false images, develop a creative background and interact with his adolescent target as someone close to her age and stage in life. Prior to the Information Age, this was not possible.

Cyberspace and the online world afford iPredator a pristine virtual reality. [Virtual reality](#) is a term that applies to computer-simulated environments that can simulate physical presence in places in the real world, as well as in imaginary worlds. For the first time in human civilization, the human predator, iPredator, has total anonymity. iPredators do not have to hide behind the proverbial bushes

and can skulk about in the dimension of cyberspace and virtual reality undetected, hidden and cloaked to perfection.

**iPreservation:** iPreservation is defined as the goal iPrey attempts to practice lowering his/her probability of becoming an iVictim at the hands of an iPredator. iPrey strives for iPreservation by practicing iPrevention. The definition of iPreservation is both a state of being and a diligent practice. When someone is consciously aware iPredator exists and they seek vulnerable iVictims, the online user experiences a sense and/or need to preserve their sanctity and safety. The motivation for iPreservation is not based on fear of iPredator, but awareness they exist. By utilizing iPrevention tactics, the online user reduces his/her potential of becoming an iVictim while accessing and interfacing with Information and Communications Technology.

Just as all living organisms have a genetic and/or instinctual need to survive, humans who interact with cyberspace and Information and Communications Technology experience iPreservation. Although iPreservation is instinctual in all online users, the level of iPreservation an online user experiences and conscious of, falls along a continuum of awareness ranging from non-existent to perpetually. For example, Internet Safety experts highly recommend online users, when posting information on their Facebook or social networking profiles to never post their full name, home address and contact information. Although most online users will understand this common sense recommendation, there still are thousands of online users who do not practice this basic Internet safety rule.

Do these online users not know how dangerous it is or simply do not care? Online users who experience the state of iPreservation would not have to be told or recommended to not disclose this information in cyberspace, because they know it is common sense not too. For those online users who do not practice iPrevention or experience iPreservation, they fall in the unfortunate category of iVictims.

The profile of the iVictim is the optimal target iPredator seeks for criminal, deviant and abusive endeavors. The iVictim is not bound to remain as such, but does not take the necessary steps required to reduce their probability of becoming a target. iVictims tend to practice denial, ignorant to Internet safety, view themselves as technologically astute or believe they are outside the purview of iPredator. iPredators believe that their criminal, deviant or abusive pursuits are fueled by their own distorted perceptions of iPreservation. For most iPredators, they believe they must harm, abuse and victimize others in order for them to thrive, and sometimes, to survive. The symbolic equation is as follows:

**iPrevention = iPreservation**

**iPrevention:** iPrevention is defined as a conscious strategy, effort and sustained approach to reducing the probability of becoming an iVictim by iPredator. The iVictim is not bound to remain as such, but does not take the necessary steps required to reduce their probability of becoming a target. iVictims do not practice iPrevention. iVictims tend to practice denial, view themselves as technologically astute, and/or outside the purview of iPredator. What online users can do to significantly reduce their probability of becoming a target of an iPredator is practice iPrevention.

iPrevention strategies involve a concerted effort to learn personal aspects and relevant demographic information that increases their chances of becoming a target. Age, gender, financial status, psychological preparedness and Internet aptitude are areas that define an online users' probability of becoming a target. Effective iPrevention requires a multi-step process for protection and insulation lasting the life of the online user who actively interfaces with Information and Communications Technology. Success with iPrevention requires acceptance the pursuit is a lifelong process.

As Information and Communications Technology will always advance, iPrevention as well must be a consistent effort. This is not to say thorough iPrevention requires advanced training in Information and Communications Technology. What is required is a willingness to practice awareness and confirmed acceptance iPredators will always be perceptive with technological advancements. Under the theory of iPrevention, the goal is not to be a step ahead of iPredator, but to be aware iPredators are always on the prowl in cyberspace and using Cyberstealth methods to stalk their prey.

Online users who practice iPrevention actively study and learn Internet safety practices, iPredator typologies, state and local laws regarding iPredators and intervention steps if the online user or their loved ones and/or their business is cyber attacked or engaged by an iPredator. By utilizing iPrevention tactics, an online user reduces his/her potential of becoming an iVictim while accessing and interfacing with Information and Communications Technology. The symbolic equation is as follows:

$$\text{iPrey} \times \text{iPrevention} = \text{iPreservation}$$

**iPredator:** A person(s) who engages in victimizing others using Information and Communications Technology motivated by deviant sexual fantasies, aggressive needs for power and control, retribution, religious/political retribution, psychiatric/psychological manifestations and/or personal/financial gain. Cyber stalkers, cyber bullies, cyber terrorists, cyber criminals and online sexual predators all use "*Cyberstealth*" afforded by the Internet, social networking and social media to stalk their prey. Under this theory, iPredator revels in his/her Internet anonymity, quickly becomes grandiose from his criminal

accomplishments and fueled by the knowledge that he/she can freely troll for his/her victims, immune from law enforcement, identification or apprehension.

By the end of 2012, Information and Communications Technology trend experts anticipate that 1.2 billion people will interface with mobile device technology and home computers on a daily basis. The frequency of digital communication and exchanges per day number in the multi-billions as Information and Communications Technology expands, improves and becomes more affordable. Without strict penal regulations, a concerted and constant law enforcement presence and a structured and sustained educational campaign for identifying iPredator, cyberspace will become a prime hunting environment for their criminal, sexually deviant, deviant, aggressive and angry pursuits.

As Information and Communications Technology gradually replaces human contact and reality based social relationships, humanity will become increasingly disconnected not realizing they increase their probability of becoming a target of iPredator. iPredator stalks quarry he/she evaluates as not practicing iPrevention or engaged in the endeavor of iPreservation. iPrevention is defined as a conscious strategy, effort and sustained approach to reducing the probability of becoming an iVictim of iPredator. iPreservation is defined as the goal iPrey attempts to practice lowering his/her probability of becoming an iVictim at the hands of iPredator.

iPrey is the population of online users, which iPredator stalks and is an inclusive term for all humanity who use the Internet, Information and Communications Technology, and Mobile Device Technology. iPredator seeks out and stalks those he/she has evaluated to be devoid of practicing iPrevention. By utilizing iPrevention tactics, the online user reduces his/her potential of becoming an iVictim, while accessing and interfacing with Information and Communications Technology. iPredators rely upon, and most often succeeds, when online users do not practice iPrevention strategies for Internet safety and cyber security. The symbolic equation is as follows:

$$\text{iPredator} + \text{iPrey} - \text{iPrevention} = \text{iVictim}$$

**iPrey:** iPrey is defined as an inclusive term for all humanity who use Information and Communications Technology. Exactly as all living predators hunt, iPredators stalk iPrey using tactical strategies to increase their probability of success. The only humans, who are not included in the category of iPrey, are those who do not interface with the Internet. With each passing year, the global expansion of Information and Communications Technology will one day include the majority of humanity ranging from industrialized countries to nations considered impoverished and/or technologically delayed. As cost decreases regarding Information and Communications Technology, the population of iPrey will steadily grow and will inevitably become all humans walking the face of the planet. Once



again, iPredator uses the same methodologies wild predators use in their hunt for food.

The only difference being iPredators do not stalk for food, survival, procreation and/or territory. iPredators stalk their quarry for deviant sexual needs, sociopathic endeavors, criminal intentions or psychological/psychiatric modus operandi. iPredators tend to be male, but female iPredators will grow steadily as Information and Communications Technology becomes more commonplace in daily living. iPrey can be low, medium, or high probability targets. Low probability iPrey are people who engage in iPrevention consciously aware there are malevolent and/or nefarious online users who will attempt to victimize them if they lower their guards down.

Medium probability targets are iPrey who engages in iPrevention consciously aware there are malevolent and/or nefarious online users who will attempt to victimize them if they lower their guards down, but cannot fully insulate themselves given their age, gender or financial status. This is not to say that the young, females or senior citizens cannot practice iPrevention or insulate themselves from victimization, but factors outside their control place them in preferred target populations of iPredators. High probability targets are people who do not practice iPrevention strategies for various reasons. High probability targets not only do not practice iPrevention, but medium probability targets, are included in iPredator's target market given their gender, age or financial status.

iPrey who are high probability targets for iPredator are defined as iVictims. iVictims are defined as people who interface with Information and Communications Technology and the Internet devoid of the necessary insulation strategies, levels of awareness, healthy forms of skepticism and structured tactical methods when interfacing with cyberspace. Unlike iVictims, iPrey have options to not only reduce their probability of becoming iVictims, but can assist their loved ones from becoming iVictims as well. iPrey utilize iPrevention strategies reducing their potential for becoming an iVictim.

iPrevention strategies are specific steps a person takes to reduce theirs or their loved ones chances of becoming a target of an iPredator. By utilizing iPrevention tactics, the online user reduces his/her potential of becoming an iVictim, while accessing and interfacing with Information and Communications Technology.

**iVictim:** iVictim is defined as an individual who interfaces with Information and Communications Technology devoid of the necessary insulation strategies, levels of awareness, a healthy form of skepticism and structured tactical methods when interacting with cyberspace. The profile of the iVictim is the optimal target iPredators seek for their criminal, deviant or abusive endeavors. The iVictim is not bound to remain as such, but does not take the necessary steps required to reduce their probability of becoming a target. iPredator is a person(s) who engages in victimizing others using Information and Communications Technology

motivated by deviant sexual fantasies, aggressive needs for power and control, retribution, religious/political retribution, psychiatric/psychological manifestations or personal/financial gain.

Cyber stalkers, cyber bullies, cyber terrorists, cyber criminals, sexual predators and white-collar fraud artists all use "*Cyberstealth*" afforded by the Internet, social networking and social media to stalk iPrey. iVictims tend to practice denial, view themselves as technologically astute and/or think they are outside the purview of iPredators. Just as all living organism predators stalk their prey, iPredators seek online users they have deemed as approachable, easily engaged and unlikely to stop their cyber attack. In the wild, predators stalk and hunt prey they have evaluated to be a highly probable target. They stalk and hunt prey they have evaluated to be the weakest and least intimidating. The most vulnerable targets for the predator and iPredator are the young, the old, the ignorant and the disabled either by physical and/or psychological deficits.

Given the vast majority of iPredators tend to be gender male, they often target female given their distorted assessment that females are less clever and/or weaker. Ignorance (not knowing), discouragement, psychologically compromised, lack of skepticism, isolation and curiosity are but a few traits iPredators look for in their hunt. It is for these reasons that children and adolescents are often prime targets. In addition to being adept at practicing Cyberstealth, iPredators are trained at sensing the mentioned attributes they deem necessary to initiate their hunt. By utilizing iPrevention tactics, the online user reduces his/her potential of becoming an iVictim when accessing and interfacing with Information and Communications Technology.

By not practicing Internet safety, online users have an increased probability of being victimized by human predators when interfacing with Information and Communications Technology. Because the iVictim is a target of iPredator, their online experiences often include higher rates of cyber bullying, cyber stalking, cyber sexual abuse, online sexual solicitations, online fraud/scams and identity theft. Just as there is controversy within the fields of criminal justice, law enforcement and criminology related to the reasons why people become and/or allow themselves to become victims, the same controversial positions applies to iVictims and cyber crime.

Given how easy it is for human predators to hide their identities when online, it becomes paramount for all people using Information and Communications Technology and the Internet to practice the necessary steps to reduce their potential from being victimized.

## NOTE TO READERS

My colleagues and I will continue to encourage colleagues, the community and proactive organizations to help alert both the public and professional sectors to what I have called the "Impending iPredator Plague." Although millions, and soon billions, of people use and rely on the Internet daily, few acknowledge the "cancer" iPredators bring to humanity if not identified and stopped.

As Information and Communications Technology continues to expand at a feverish pace coupled with seemingly daily introductions of new technology, ever-increasing obstacles will challenge humanity. Already, online users have been confronted by the ever-increasing detriments of having incredible amounts of information, which can be obtained, exchanged and spread at incredible speed. Terms such as Digital Reputation, Digital Footprint, Digital Citizenship and other similar concepts are now part of our social media interactions and concerns.

Adults, businesses, children, celebrities, politicians and every other facet of our communities must now be wary. Online users now have to be concerned about what information they have shared online in the past and what information they have never disclosed, but now accessible to others. In addition to personal information being disclosed, online users and businesses must now become educated and cautious about Social Engineering, Social Intelligence, Internet Libel and Internet Defamation.

From a nationalistic perspective, industrialized nations must now allocate increasing amounts of time, money, work force and strategic planning to address the growing concerns of homeland security, cyber terrorism and cyber warfare all due to social media and the speed and magnitude of Information and Communications Technology. In addition to the cyber threats to our national security, it is fair to assume iPredators and groups of iPredators will become willing activists attempting to access and design larger and more deadly forms of cyber aggression.

Social science experts and educators have attempted to enlighten and warn the global community, but their impact to date pales in comparison to the wrath and inevitable growth of the threat of iPredators and the growing number of iPredator groups. This writer and his future proactive associates and organizations will attempt to motivate society before iPredators become a common fixture in the fast growing Internet global community. Cyberspace represents a new dimension and a new territory for social exploration. Unfortunately, iPredators patiently wait in the shadows of this dimension with bated breath.

## iPREDATOR INC.

iPredator Inc. was founded in September 2011 to provide educational and advisory products & services to consumers and organizations on Cyber Bullying, Cyber Stalking, Child Predators, Cyber Crime, Internet Defamation, Cyber Terrorism and the new fields of ICT Forensic Psychology & ICT Psychology they are pioneering. Created by a New York State licensed psychologist and certified forensic consultant, Dr. Michael Nuccitelli, their goal is to reduce victimization, abuse, theft and disparagement from online assailants.

In addition to assisting citizens, iPredator Inc.'s mission is to initiate a nationally sustained educational & awareness campaign with the help of private, state and federal agencies. In May 2012, iPredator Inc. launched their website, [www.iPredator.co](http://www.iPredator.co) along with their forensics blog, [Dark Psychology](#). On their website, they offer an enormous free resource library for site visitors covering the vast range of Cyber Predators, Internet Safety, Cyber Security, ICT Psychology, Forensic Psychology and Criminal Psychology.

As Chief Operating Officer, Dr. Nuccitelli became interested in the psychology and profiling of those who use information and communications technology to abuse, steal, taunt and victimize others online in 2009. In 2012, Dr. Nuccitelli and his team of expert consultants grew even more determined to develop victimization prevention & intervention strategies for vulnerable online users utilizing education, investigation, legal, law enforcement and information technology experts.

At the center of iPredator Inc.'s products, services and investigation strategy is Dr. Nuccitelli's theoretical construct, iPredator. As a member and consultant to the [American College of Forensic Examiners International](#), iPredator was the feature article in their 2011 winter issue of [The Forensic Examiner](#) published quarterly. Since 2009, Dr. Nuccitelli has dedicated himself to learning the psychological composition of those who are engaged in online malevolent activities. His definition of iPredator is as follows:

**iPredator**: A child, adult or group who engages in the exploitation, victimization, stalking, theft or disparagement of others using information and communications technology (ICT.) iPredators are driven by deviant fantasies, desires for power and control, retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance or personal and financial gain. iPredators can be any age, either gender and not bound by economic status, race or national heritage.

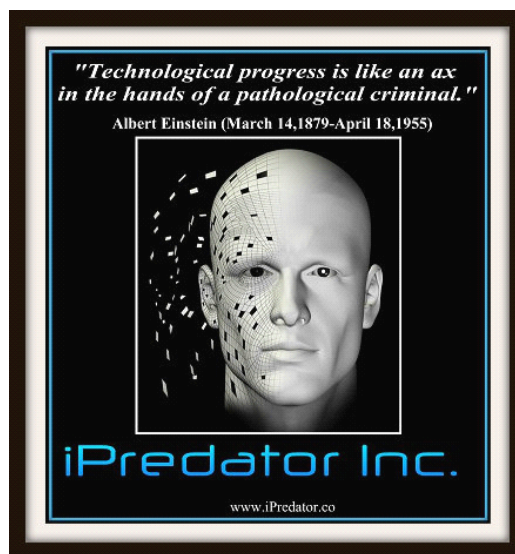
Dr. Nuccitelli and his colleagues have compiled an enormous database leading to iPredator Inc.'s resource library available at no charge to all site visitors. Having read, reviewed and compiled these links, websites and resources, he went on to

develop the IPI Assessment Collection & iPredator Checklist Collection designed for parents, businesses, educators, healthcare professionals, teens, adults and public figures offered on their website to take online and/or purchase.

The IPI Assessment Collection & iPredator Checklist Collection address cyber bullying, cyber crime, cyber stalking, cyber terrorism, digital reputation, social media, corporate disparagement and cyber predators. Interested parties can also purchase the licenses to these assessments to use for their own endeavors to educate and assess their communities, organizations and businesses in their online activities and ICT safety practices.

Concurrent with these assessments, iPredator Inc. offers a unique educational & advisory-based membership service called iPredator Protected. iPredator Protected functions to educate, advise and assist their members with the appropriate strategies for prevention, intervention, investigation and guidance if targeted by an iPredator. iPredator Inc. services include trainings, educational seminars, phone consultations and advisory, investigation, forensic and ICT Forensic Psychology services for law enforcement, attorneys and court systems. iPredator Inc. also offers trainings on ICT Psychology and Digital Reputation Management for businesses and the general public.

iPredator Inc. retains and consults with regional and national attorneys, law enforcement, ICT security experts, criminal investigators and the American College of Forensic Examiners International. Law enforcement, the legal system, community organizations and national activist organizations support iPredator Inc., their mission and the products, services and valuable information they share on their website, [www.iPredator.co](http://www.iPredator.co).



## iPREDATOR RESOURCE LINKS

Aldous Huxley: <http://www.huxley.net/>  
Alfred Adler: <http://www.muskingum.edu/~psych/psycweb/history/adler.htm>  
American College of Forensic Examiners International: <http://www.acfei.com/>  
Botnets, Cybercrime and Cyberterrorism:  
<http://www.au.af.mil/au/awc/awcgate/crs/rl32114.pdf>  
Brian Harvey, University of California Berkley:  
<http://www.cs.berkeley.edu/~bh/hacker.html>  
Center for Cyber Research: <http://www.afit.edu/en/ccr/index.cfm>  
Children's Hospital Boston:  
<http://web1.tch.harvard.edu/az/Site1561/mainpageS1561P0.html>  
C.I.A.: <https://www.cia.gov/>  
Cyber Citizenship Partnership:  
<http://www.cybercitizenship.org/crime/crime.html>  
Cyber Criminal Activity: Methods & Motivations:  
[http://www.cs.washington.edu/education/courses/csep590/05au/whitepaper\\_turnin/CyberCriminalActivityFinalDraft.pdf](http://www.cs.washington.edu/education/courses/csep590/05au/whitepaper_turnin/CyberCriminalActivityFinalDraft.pdf)  
Cyber Criminals Most Wanted: <http://www.ccmstwanted.com/>  
Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws: <http://www.law.missouri.edu/lawreview/docs/72-1/Goodno.pdf>  
Cyber Terrorism:  
<http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>  
Cisco Visual Networking Index Global IP Traffic Forecast, 2010-2015 Update:  
<http://www.youtube.com/watch?v=3XAqOVD0u7k>  
Cisco VNI Forecast:  
[http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white\\_paper\\_c11-520862.html](http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html)  
CRS Report for Congress:  
[http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30735\\_06192001.pdf](http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30735_06192001.pdf)  
Cyber Warfare: <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>  
Cornell University Law School:  
<http://www.law.cornell.edu/uscode/text/18/1512>  
Dark Psychology: <http://darkpsychology.co/>  
Department of Homeland Security: <http://www.dhs.gov/index.shtm>  
Dictionary.com: <http://dictionary.reference.com/browse/mark>  
Director of National Intelligence: <http://www.dni.gov/>  
Examiner.com:  
<http://www.examiner.com/article/criminals-casing-homes-and-stores>  
Educause: <http://net.educause.edu/ir/library/pdf/ELI7008.pdf>  
FBI.gov:  
<http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism>  
Forensic Examiner: <http://www.theforensicexaminer.com/>



George Orwell: [http://www.george-orwell.org/l\\_biography.html](http://www.george-orwell.org/l_biography.html)

GfK: <http://www.gfkamerica.com/>

Glenn Stutzky M.S.W., School of Social Work, Michigan State University: [http://www.ippsr.msu.edu/Documents/Forums/2006\\_Mar\\_CYBER\\_BULLYING\\_INFORMATION\\_2006%20--%20Provided%20by%20Mr.%20Glenn%20Stutzky.pdf](http://www.ippsr.msu.edu/Documents/Forums/2006_Mar_CYBER_BULLYING_INFORMATION_2006%20--%20Provided%20by%20Mr.%20Glenn%20Stutzky.pdf)

ICT Literacy: <http://www.icliteracy.info/rf.pdf/impact-digital-tech.pdf>

Internet Crime Complaint Center: <http://www.ic3.gov/default.aspx>

Internet Safety Project: <http://www.internetsafetyproject.org/wiki/william-francis-melchert-dinkel>

Indiana University Information Technology Services: <http://kb.iu.edu/data/arsf.html>

Institute for Security Technology at Dartmouth College: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA395300>

International Telecommunications Union: <http://www.itu.int/en/Pages/default.aspx>

Internet World Stats: <http://www.internetworldstats.com/stats.htm>

iPredator Inc.: [www.iPredator.co](http://www.iPredator.co)

JESS3: <http://www.slideshare.net/jess3/the-geosocial-universe-version-2-process-deck>

Library of Congress: <http://www.loc.gov/search/?q=information+and+communications+technology&fa=digitized%3Atrue&st=gallery>

McAfee: <http://www.mcafee.cc/Bin/sb.html>

National Center for Missing & Exploited Children: [http://www.missingkids.com/en\\_US/publications/NC70.pdf](http://www.missingkids.com/en_US/publications/NC70.pdf)

National Criminal Justice Reference Service: <https://www.ncjrs.gov/internetsafety/cyber.html>

National Cyber Security Alliance: <http://staysafeonline.mediaroom.com/index.php?s=27478>

National Geographic: <http://animals.nationalgeographic.com/animals/mammals/wildebeest/>

National Security Agency: <http://www.nsa.gov/>

National Sex Offender Public Website: <http://www.nsopw.gov/Core/Portal.aspx?AspxAutoDetectCookieSupport=1>

Neuromancer: <http://workingtropes.lcc.gatech.edu/wiki/index.php/Neuromancer>

New Scientist: <http://www.newscientist.com/article/dn13687-evolution-myths-evolution-promotes-the-survival-of-species.html>

Nielsen Online: <http://www.nielsen.com/content/corporate/global/en.html>

N.J.S.A.: <http://www.judiciary.state.nj.us/criminal/charges/bias3.pdf>

Norton by Symantec: [http://us.norton.com/content/en/us/home\\_homeoffice/html/cybercrimereport/](http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/)

PC Mag:

[http://www.pcmag.com/encyclopedia\\_term/0,2542,t=Smartphone&i=51537,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t=Smartphone&i=51537,00.asp)

Permanent Select Committee on Intelligence: <http://intelligence.house.gov/>

Phenomenological Psychology:

<http://phenomenologicalpsychology.com/2009/10/alfred-adlers-concept-of-social-interest/>

Profile of a Pedophile, Charles Montaldo:

<http://crime.about.com/od/sex/p/pedophile.htm>

Psychology Today: <http://www.psychologytoday.com/basics/narcissism>

PubMed Health: <http://www.ncbi.nlm.nih.gov/pubmedhealth/PMH0001941/>

Ray Bradbury: <http://www.raybradbury.com/>

Read, Write, Think:

[http://www.readwritethink.org/files/resources/lesson\\_images/lesson926/DefinitionCharacteristics.pdf](http://www.readwritethink.org/files/resources/lesson_images/lesson926/DefinitionCharacteristics.pdf)

Readiness for the Networked World:

<http://cyber.law.harvard.edu/readinessguide/guide.pdf>

Science Daily:

[http://www.sciencedaily.com/news/computers\\_math/virtual\\_reality/](http://www.sciencedaily.com/news/computers_math/virtual_reality/)

Socialight: [http://uberthings.com/mobile/intro\\_to\\_mobile.pdf](http://uberthings.com/mobile/intro_to_mobile.pdf)

Stanford School of Medicine: <http://ocd.stanford.edu/about/>

Stop Bullying.gov: <http://www.stopbullying.gov/cyberbullying/index.html>

Stop Cyberbullying:

[http://www.stopcyberbullying.org/what\\_is\\_cyberbullying\\_exactly.html](http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html)

Stop Cyberbullying:

[http://www.stopcyberbullying.org/how\\_it\\_works/cyberbullying\\_by\\_proxy.html](http://www.stopcyberbullying.org/how_it_works/cyberbullying_by_proxy.html)

Symantec Internet Security Threat Report, Volume 16:

[http://www.symantec.com/about/news/resources/press\\_kits/detail.jsp?pkid=threat\\_report\\_16](http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threat_report_16)

Tech Target: <http://searchsecurity.techtarget.com/definition/black-hat>

Tech Target: <http://searchsecurity.techtarget.com/definition/white-hat>

Tech Target: <http://searchsecurity.techtarget.com/definition/stealth>

The Free Dictionary by Farlex:

<http://legal-dictionary.thefreedictionary.com/invasion+of+privacy>

The Research Press:

[http://www.umassmed.edu/uploadedFiles/eap2/resources/Families\\_and\\_Parenting/parentsguidecyberbullying.pdf](http://www.umassmed.edu/uploadedFiles/eap2/resources/Families_and_Parenting/parentsguidecyberbullying.pdf)

T.I.A.: <http://www.tiaonline.org/>

United States Cyber Command:

[http://www.defense.gov/home/features/2010/0410\\_cybersec/](http://www.defense.gov/home/features/2010/0410_cybersec/)

United States Department of Justice:

<http://www.justice.gov/criminal/cybercrime/>

U.S. Department of Justice Federal Bureau of Investigation:

<http://www.fbi.gov/stats-services/publications/parent-guide/parentsguide.pdf>

U.S. Legal: <http://definitions.uslegal.com/t/tampering-with-evidence/>

U.S. Legal: <http://definitions.uslegal.com/c/computer-hacking/>

Violence Prevention Project:

<http://www.fresnostate.edu/vpp/stalking/cyberstalking.shtml>

Webopedia: [http://www.webopedia.com/TERM/D/digital\\_footprint.html](http://www.webopedia.com/TERM/D/digital_footprint.html)

Webopedia: [http://www.webopedia.com/TERM/W/World\\_Wide\\_Web.html](http://www.webopedia.com/TERM/W/World_Wide_Web.html)

Wikipedia: <http://en.wikipedia.org/wiki/Anger>

Wikipedia: <http://en.wikipedia.org/wiki/Dystopia>

Wikipedia: [http://en.wikipedia.org/wiki/Fahrenheit\\_451](http://en.wikipedia.org/wiki/Fahrenheit_451)

Wikipedia: <http://en.wikipedia.org/wiki/Greed>

Wikipedia: <http://en.wikipedia.org/wiki/Guilt>

Wikipedia: [http://en.wikipedia.org/wiki/Inferiority\\_complex](http://en.wikipedia.org/wiki/Inferiority_complex)

Wikipedia: [http://en.wikipedia.org/wiki/Information\\_Age](http://en.wikipedia.org/wiki/Information_Age)

Wikipedia: [http://en.wikipedia.org/wiki/Little\\_Red\\_Riding\\_Hood](http://en.wikipedia.org/wiki/Little_Red_Riding_Hood)

Wikipedia: <http://en.wikipedia.org/wiki/Remorse>

Wikipedia: <http://en.wikipedia.org/wiki/Sextortion>

Wikipedia: [http://en.wikipedia.org/wiki/Signature\\_crime](http://en.wikipedia.org/wiki/Signature_crime)

Wikipedia: [http://en.wikipedia.org/wiki/Social\\_network](http://en.wikipedia.org/wiki/Social_network)

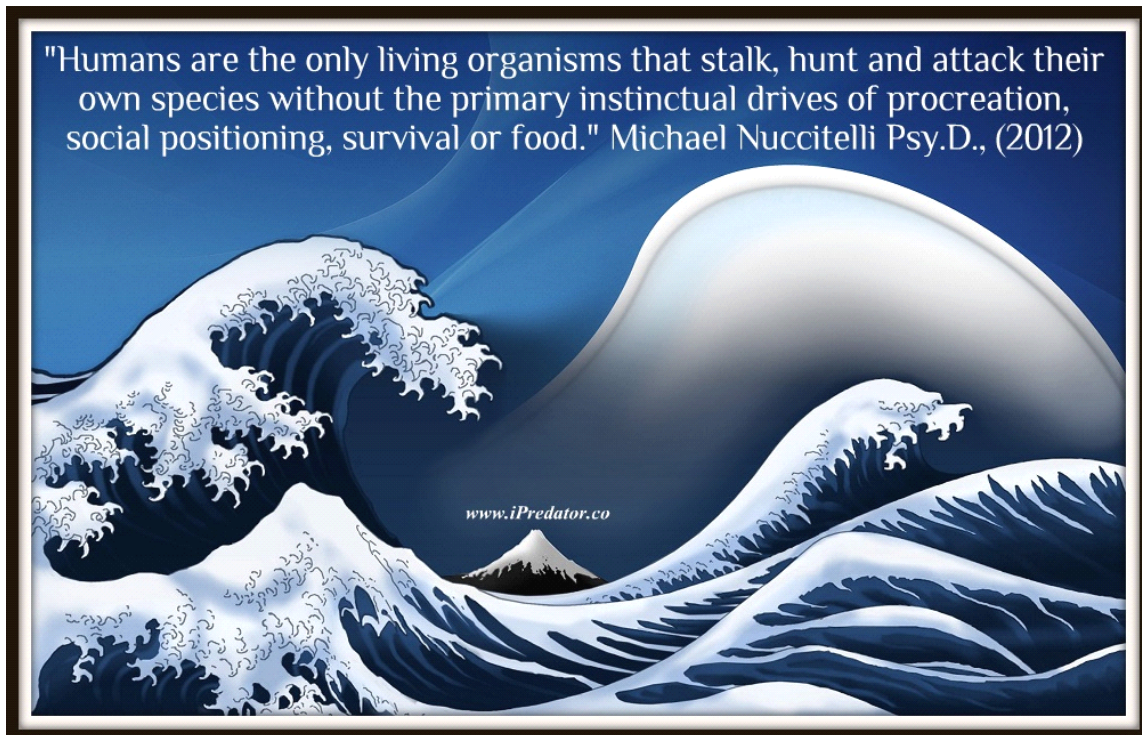
Wikipedia: [http://en.wikipedia.org/wiki/Troll\\_\(Internet\)](http://en.wikipedia.org/wiki/Troll_(Internet))

Wikipedia: [http://en.wikipedia.org/wiki/Virtual\\_reality](http://en.wikipedia.org/wiki/Virtual_reality)

William Gibson: [http://en.wikipedia.org/wiki/William\\_Gibson](http://en.wikipedia.org/wiki/William_Gibson)

WTHITV.com:

<http://www.wthitv.com/dpp/video/video-richard-finkbiner-sexstortion-press-meeting>



***PROTECT, PREVENT & PREVAIL OVER IPREDATORS***