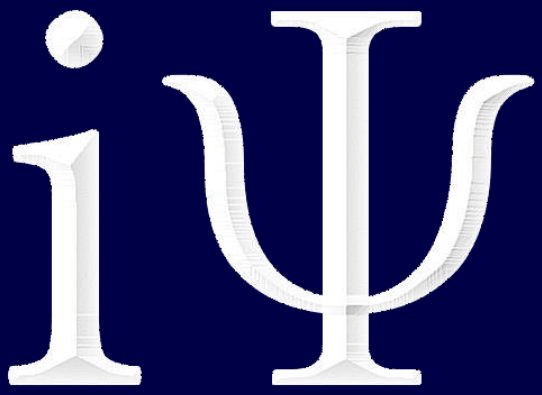
IPREDATOR

Dark Side of Cyberspace Concept

Edited & Revised
(hyperlinked copy)



Michael Nuccitelli, Psy.D.
NYS Licensed Psychologist
New York City, New York
Phone: (347) 871-2416
Website www.ipredator.co

iPredator Table of Contents

I. iPredator Concept ……1-25

II. iPredator Formal Definition ……2-3

III. iPredator Typologies ……26-29

IV. iPredator Relevant Concepts ……29-35

V. Author Biography ……36

VI. Sources Cited ……37

Information and Communications Technology (ICT), social media, and cyberspace itself has the uncanny ability to tap into our perceptual world and distort our interpretations of oneself and others. For those who experience gratitude, it helps the human condition and community. For those who suffer wrath, anguish, or ingratitude? Condemnation of self and society becomes the weapon.

Original Version Authored by Michael Nuccitelli, Psy.D. December 2009
Edited & Revised Version Authored by Michael Nuccitelli, Psy.D. December 2019
Copyright © 2019 Michael Nuccitelli, Psy.D., All Rights Reserved.

IPREDATOR

The Dark Side of Cyberspace in the Information Age

by

Michael Nuccitelli, Psy.D.

(Edited & Revised)

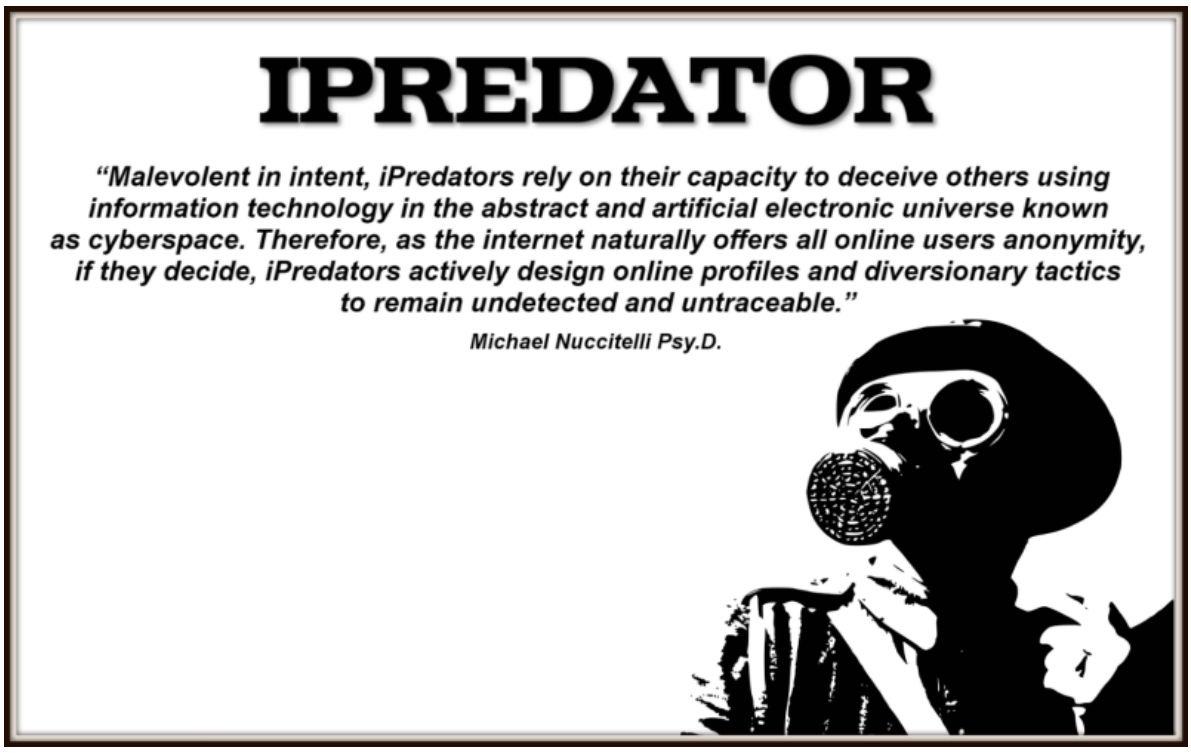
As a licensed clinical psychologist with extensive experience in both criminology and abnormal psychology, this writer has formulated a psychological, sociological, and criminological profile for the growing dimension known as the dark side of cyberspace. I have named the theoretical paradigm of this modern-day criminal and psychological reprobate iPredator. This new breed of human predator uses Information and Communications Technology (ICT) to profile, investigate, track, and attack their human prey. The typologies and behaviors of iPredator include cyberbullying, cyber harassment (adult cyberbullying), cybercrime, cyberterrorism, cyberstalking, online sexual predation, internet trolling, and online child pornography (both consumption and distribution).

Vital to understanding the theoretical core of iPredator is that they are variants of classical criminals, deviants, and nefarious entities. ICT and the information age have created a new dimension leading to an entirely new population of humanity engaged in malevolent, harmful, and deceptive practices. ICT and cyberspace are not just tools used by the psychopath, deviant, narcissist, or classic criminal, but part of a new generation that will be permanent fixtures to humanity for centuries to follow.

Cyberspace allows our darkest fantasies to be fueled by the like-minded. When validated by others, they are one step closer to becoming reality.

The term iPredator is a global concept designed to include any child, adult, business entity or organized group who uses ICT to harm, abuse, steal from, assault, or defame other ICT users. Also included in this concept are people who benefit from technocentric victimization but are not the principal perpetrators, such as criminals who engage in the sale and profit

of online child pornography. As ICT advances and humanity becomes more dependent upon information technology, it is inevitable the typologies of iPredator will expand as well.



iPredator Formal Definition

iPredator: a person, group, or nation who, directly or indirectly, engages in exploitation, victimization, coercion, stalking, theft, or disparagement of others using Information and Communications Technology (ICT). iPredators are driven by deviant fantasies, desires for power, control, and retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance, or personal and financial gain. iPredators can be any age or gender and are not bound by economic status, race, religion, or national heritage. Their sole requirement to get started in this dark dimension is an internet connection.

Central to the concept is the premise that information age criminals, deviants, and the violently disturbed are psychopathological classifications new to humanity. Whether the offender is a cyberbully, cyberstalker, cyber harasser, cybercriminal, online sexual predator, cyberterrorist, internet troll, online child pornography consumer/distributor, or a person engaged in internet defamation or nefarious online deception, they fall within the scope of iPredator. The three criteria used to define an iPredator include:

- A self-awareness of causing harm to others, directly or indirectly, using ICT;
- The usage of ICT to obtain, tamper with, exchange and deliver harmful information;

- A general understanding of cyberstealth used to engage in criminal or deviant activities or to profile, locate, stalk, and engage a target.

Unlike human predators prior to the information age, iPredators rely on the multitude of benefits offered by ICT. The primary differentiators of this very modern kind of predation are also threefold: the unlimited *distance* over which data can be conveyed, the *immediacy* with which the data can be conveyed, and the unlimited *scope* of data that can be conveyed. The importance of these three vectors of capability cannot be overstated. In pre-information age societies, by contrast, a predator's malicious activity was essentially local, slow-moving, and technologically constrained; the predator was limited to the area he could cover by car, to use an emblematic example, needed careful wooing or "casing" of his victim, and was restricted by the limitations of relatively crude technologies like the telephone.

In the abstract and artificial electronic universe known as cyberspace, none of these restrictive qualifiers obtain. Furthermore, there is a fourth advantage that ICT offers iPredators: *anonymity*. On the internet it is easy for iPredators to actively design online profiles and diversionary tactics to remain undetected and untraceable.

Cyberstealth, an important sub-tenet of iPredator, is a covert method by which iPredators attempt to set up 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 iPredator Victim Intuition (IVI). An iPredator's IVI is their aptitude to sense a target's ODDOR (Offline Distress Dictates Online Response), online and offline vulnerabilities, psychological weaknesses, and technological limitations, increasing their success of a cyber-attack with minimal ramifications.

If you spend too much time in cyberspace without calming and restorative interludes, you are bound to project your insecurities and skewed perceptions upon others.

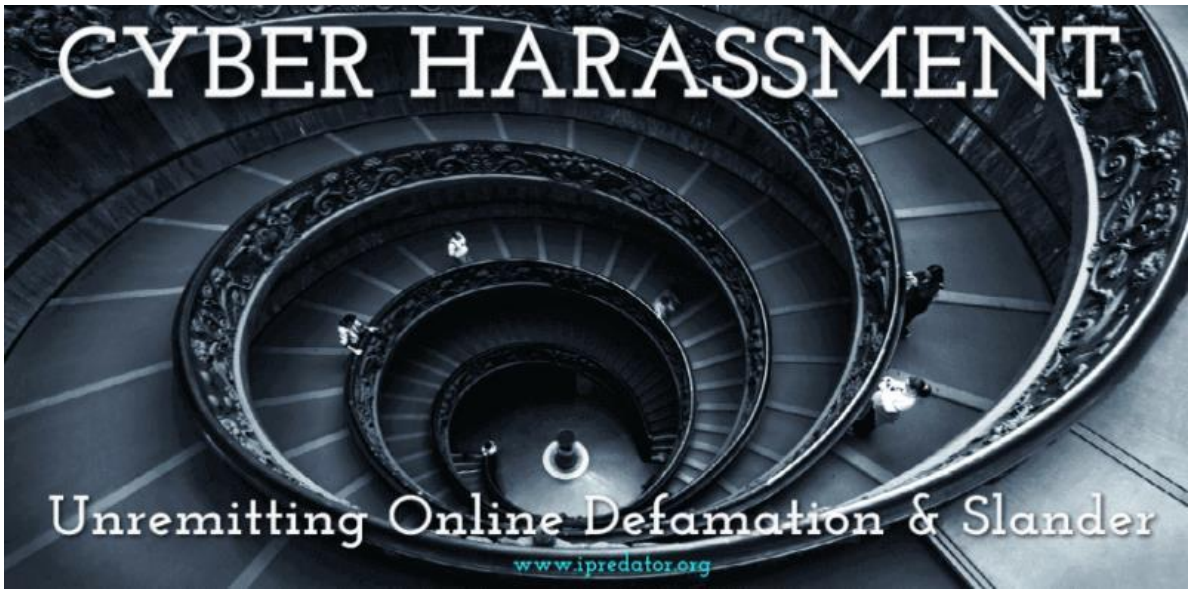
The Dark Side of Cyberspace

The abundance of real-life iPredators with their arrests and prosecutions provide a harrowing look into their methods of operation. In one case, the owner of a small internet service provider in Indiana was charged with blackmailing children into performing sexually explicit acts over a webcam. The allegations involved two 14-year-old boys, but the FBI found thousands of sexually explicit images and videos on the perpetrator's computer, suggesting hundreds of other victims were involved in his extortion scheme. Using a fake

identity, the perpetrator frequented anonymous video-chat websites to find children online. He used "fake webcam" software to display pornographic videos claiming to be live feeds of himself from his webcam.

While showing these videos, the perpetrator encouraged his victims to engage in sexually explicit or suggestive activity themselves, which he secretly recorded. He then threatened to make these videos available to their parents, friends, and coaches. He also threatened to post their images on pornographic websites. The perpetrator was quoted as telling one victim that he was a "hacker" who knew how to remain anonymous. "Only I have this link," the perpetrator wrote to one victim; "You want to play this game, or you want to be a gay porn star?" To another, he acknowledged, "Yes, it is illegal and I'm OK with that," warning that "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 terror the perpetrator's threats caused his victims was chillingly revealed in the transcript of an email message one of the boys sent to him, 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. The presence of hundreds of alleged victims makes the Indiana investigation and prosecution among the larger, if not largest, sextortion case prosecutors have ever undertaken in the United States.



Another telling case study is of a man eventually convicted on two counts of contributing to the suicide of two people, one a 32-year-old Englishman who hanged himself, the other an 18-year-old Canadian woman who jumped to her death into a frozen river. The perpetrator

was the first person charged and convicted of assisted suicide using the internet. State prosecutors presented evidence the perpetrator posed online as a 28-year-old, depressed female nurse engaged in encouraging, recommending, and aiding young adults to commit internet suicide.

This perpetrator frequented suicide chat rooms under the names "Li Dao," "Cami D," and "Falcongirl." Obsessed with hanging by suicide, he searched out potential suicide victims online. Court documents said he told police he destroyed these lives simply for the "thrill of the chase." He acknowledged taking part in online chats about suicide with an estimated twenty people, and entered into felonious suicide pacts with ten, five of whom he believed succeeded. Central to his deviant obsession was encouraging his victims to stream their suicides live on webcam for him to watch.

Internet predation takes many forms and can be particularly pernicious when used in conjunction with digital recording devices and social media. Consider the case of the harassment and subsequent suicide of a New Jersey college student whose roommate and a fellow hallmate used an instant messaging software application to view, without his knowledge, the student kissing another man. The roommate later tried to view the student's sexual encounters a second time and drew attention to the event in 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, the student jumped to his death from the George Washington Bridge.

The roommate ended up facing fifteen charges, including invasion of privacy and witness tampering, with evidence of bias intimidation attached to some of the charges. The roommate was found guilty of all fifteen counts, including all four bias intimidation charges, but 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 focused the United States on the victimization of LGBT youth and the growth and negative impact of cyberbullying. Public figures, including Ellen DeGeneres and President Barack Obama, spoke out about the tragedy and New Jersey legislators subsequently enacted the nation's toughest law against bullying and harassment.

Welcome to the unseemly and perverse world of cyberstalkers, the digitally depraved and malevolent iPredators.

iPredator and ICT

Again, the three criteria used to define an iPredator include:

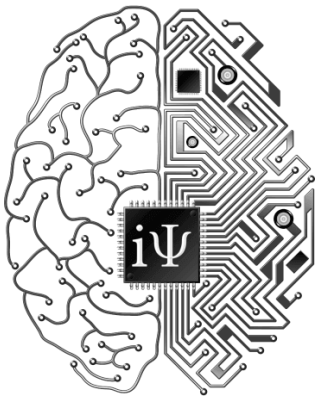
- A self-awareness of causing harm to others, directly or indirectly, using ICT;

- The intermittent to frequent usage of ICT to obtain, exchange and deliver harmful information;
- A general understanding of cyberstealth to engage in criminal or deviant acts or to profile, identify, locate, stalk, and engage a target.

Of the three measures used to define an iPredator, the first criteria "A self-awareness of causing harm to others, directly or indirectly, using ICT" can be difficult to confirm unless the online user has personally assessed their own motivations. When others try to evaluate if someone is an iPredator using factor one, they must use circumstantial evidence that supports the conclusion that the ICT user is aware of the direct or indirect harm they are causing others using ICT.

If a minor meets the three criteria, they are defined as iPredators, just as adults, and considered to be just as dangerous and sinister as adults. In relationship to cyberbullying, there is a small percentage of young ICT users who are either ignorant of the harm they are causing another child or genuinely believe they are joking. Another small sub-group of ICT offender who do not meet the iPredator criteria are those suffering from a verifiable psychiatric disorder (Schizoaffective Disorder, Bipolar Disorder, Schizophrenia, etc.) as defined by the *Diagnostic and Statistical Manual of Mental Disorders* published by the American Psychiatric Association.

Online users who suffer from severe psychiatric disorders may not be aware that their ICT activities are causing the recipient significant distress. Of the total pool of suspected and genuine iPredators, an estimated 1-3% of ICT perpetrators are not aware of the direct or indirect harm they are inflicting upon their victims and do not fit the criteria for iPredator. Although the American judicial system casts a large net for defining the intent and culpability of a defendant, this proverbial net is decreased when defining an iPredator. If an ICT user causes others harm, engages in ICT activities, and uses the veil of anonymity afforded to all online users, they are both culpable for their actions and defined as an iPredator.



iPredator Victim Intuition (IVI)

A fourth criterion, not included in the triad defining an iPredator, is what this writer has termed iPredator Victim Intuition (IVI), which is reserved for seasoned iPredators. IVI is the aptitude to sense a target's online vulnerabilities, weaknesses, and technological limitations, increasing the iPredator's success with minimal ramifications. Through practice and learning, iPredators develop the skill of being able to sense, by intuition, when an ICT user will make a successful target.

Just as classic criminals can "case" a home or a sexual predator choose the most vulnerable child to abduct, the iPredator can identify a potential victim using the information they compile from a variety of online and offline sources and contacts. Based on the typology of iPredator, the areas they investigate in their strategy of targeting a victim include:

- The amount of personal information a potential target reveals using ICT;
- The frequency with which a potential target shows their contact information using ICT;
- The content of the information a potential target discloses using ICT;
- The lack of internet safety measures a potential target institutes online;
- The potential target's willingness to discuss sensitive issues including sexual topics, financial information, their physical location, parental or adult monitoring of their ICT activities, experiences of distress at home, work, and school, and interpersonal or intrapersonal issues;
- The amount of time the potential target spends online;
- The type of information a potential target reveals on their social networking profiles;
- The potential target's offline and ICT-absent demeanor;
- The potential target's ignorance of, or unwillingness to push back against, negative information being generated by an iPredator;
- The potential target's probability of not having social system support, legal and law enforcement support, or knowledge of intervention strategies if attacked via ICT;
- The quantity and themes of images and videos a potential target shares using ICT;
- The pattern of "likes" and "dislikes" an ICT user discloses on their social networking site profiles;
- The frequency with which a potential target changes their profile images and information on their social networking site profiles;
- Images and videos showing the potential target's economic status, the layout of their residence, and material objects they or their loved ones own;
- Images, videos, and posts published online of the potential target's lifestyle;
- Images, videos, and posts dispersed using ICT of the potential target's needs, wishes, and desires;
- Images, videos, and posts publicized using ICT suggesting the potential target is suffering from psychological and/or psychosocial dysfunction.

Soon, information will become the most lethal and feared weapon; more valuable than diamonds, intoxicating like morphine.

Although there are other factors an iPredator uses in their repertoire of performing IVI, the seventeen factors listed are recommended for evaluation by all online users to reduce their chances of becoming an iPredator target. Not included in these factors is the unfortunate reality of being targeted by an iPredator as part of a mass trolling scheme called "Phishing." This situation occurs most often in cybercrime when the potential target receives an email asking them to open an attachment or is gulled into giving personal information.

An iPredator's IVI acumen is based on practice, experimentation, understanding of human behavior, and knowledge of internet safety practices and ICT. In the same way a locksmith is skilled at opening a variety of locks, an iPredator is adept at choosing a target they have concluded will not cause them to be named, apprehended, or punished. Criminologists have a useful theory called routine activity theory, which "argues that opportunities for victimization occur when a motivated offender, suitable target, and absent or ineffective guardianship converge in time and space." The authors of an essay in the *American Journal of Criminal Justice* observe that

> "those in abusive relationships may feel unable to affect their risk of victimization due to a perceived lack of control over the situation or their environment generally. This issue may also be evident in some forms of cybercrime victimization, as the very nature of the Internet can impact individuals' victimization risks in ways that may be otherwise hidden or hard to appreciate. Certain offenses such as online harassment may be directly influenced by both an individual's online routine activities as well as their individual attitudes and behaviors."

An iPredator's IVI falls upon a continuum of dexterity, whereby some iPredators are advanced in their IVI skills and others are novices. Whether the iPredator is advanced or novice in their IVI acumen, the fact that they engage in developing IVI makes them potentially dangerous.

In addition to having IVI, the iPredator practices cyberstealth using multiple covert strategies. In fact, one of the key criteria used to define an iPredator is a general understanding of how cyberstealth can be used to engage in criminal or deviant acts or to profile, find, stalk, and engage a target. Although cyberstealth skills also lie on a continuum, advanced iPredators almost never engage in the haphazard approach of targeting a victim without trying to hide their identity. In contrast, cyberbullies, ex-partners, ex-employees, angry or self-righteous online users, internet trolls, organized groups with political, religious, moralistic agendas, child molesters, pedophiles and highly narcissistic online users occasionally do not try to hide their identities.

Cyberstealth

Cyberstealth is a strategy reserved for iPredators who look to hide their identities and nefarious objectives online. Cyberstealth, a concept formulated along with iPredator, is a term used to define a method or strategy by which iPredators devise tactics to set up and sustain complete anonymity while they troll and stalk an online target. In addition to a stratagem, cyberstealth is a reality of ICT that humanity often fails to fathom, leading some ICT users to become high-probability targets. Cyberstealth is a learned behavior that becomes more advanced with practice, trial and error, and experimentation.

Some iPredators even seek the advice and consultation of other iPredators to hone their skills, especially in the realm of hackers, who actively seek insight from other hackers to advance their knowledge base. Although hackers tend to be considered by the general mainstream as villainous, there are two distinct groups defined by their motivations. "Black Hat Hackers" engage in nefarious and malevolent online activities. "White Hat Hackers" are ICT security experts.

Cyberstealth used by iPredators ranges from negligible to extraordinarily complex and multifaceted.

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 ICT products and services focused on hiding an ICT user's identity and the ability to engage in anonymous surveillance. In addition to a learned behavior, cyberstealth may also include an inherited aptitude, ability, or skill set, just as some people have exceptional skills even though they are new to a craft. The

rationale for using "stealth" in the suffix of cyberstealth serves to remind ICT users of the primary intent fueling many iPredators.

Their motivation is to hide their identity or goal by designing fictive online profiles, identities, tactics, and methods to ensure their identities still are concealed, reducing recognition and castigation. Therefore, as the internet and ICT naturally offer all users anonymity, iPredators actively design profiles and diversionary tactics to remain undetected and untraceable. For most ICT users, anonymity is an *option*, a method of viewing the internet that can be toggled off or on, depending on whether the user wants to engage secretly or under their real persona. In many online arenas, such as online dating,social media "branding" of oneself as a performer or expert, or job searching and professional development, a vibrant and specific identification is central to the entire process. For the iPredator, in contrast, there is never any reason to be authentic online; anonymity is not an option but a *necessity*. For the iPredator, existence equals stealth.

According to 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; the quality or characteristic of being furtive or covert." Cyberstealth is a covert method by which iPredators can create 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.

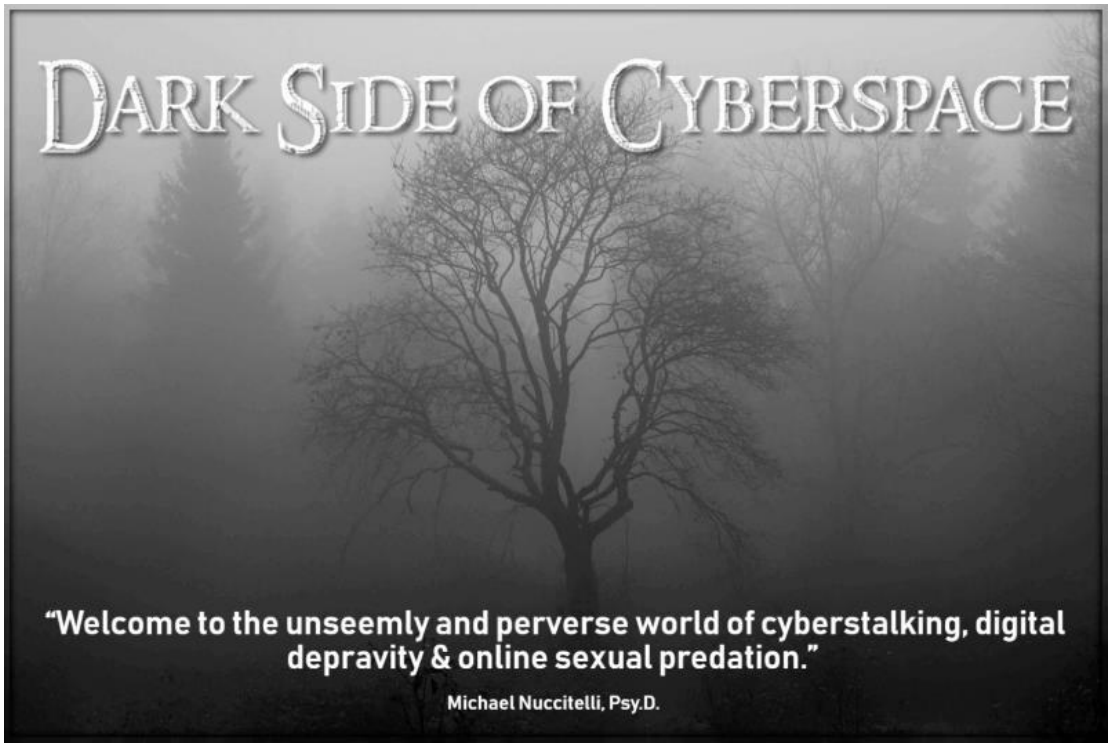
When profiling or investigating an iPredator, their level of cyberstealth complexity, digital footprint, victim preferences, ICT skills, and behavioral patterns are used to figure out who they are. Assessment of an iPredator's cyberstealth tactics and digital footprint can aid authorities in their profiling, identification, and apprehension. Just as classic criminal profiles have signatures used to apprehend them, iPredators have digital signatures as well. The goal of the United States and all industrialized nations is to stop the growth of iPredators by educating its citizens on their tactics and strategies. Of course, some nations use iPredators for their own goals, and have set up extensive operations realizing it to be another way to their goals whether using the same skill set as the individual iPredator but with extensive support from the government.

The Changing Digital Landscape

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; the information age has spread to all corners of the planet. The pace of new technology introductions and number of internet users will continue to grow at an accelerated rate is accepted as a priori fact.

Although ICT benefits far outweigh the 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 belief, humanity also does not heed the warnings of prophetic authors of the past century who sketched chilling glimpses of a dystopian society on the edge of destruction and authoritarian control due to utter reliance upon ICT.

Scholar Dinah Birch defines dystopia as "a modern term invented as the opposite of utopia, and applied to any alarmingly unpleasant imaginary world, usually of the projected future. The term is also applied to fictional works depicting such worlds. A significant form of science fiction and of modern satire." In a society of complete ICT dependency, personal freedoms are banished, and citizens are left at the mercy of the government's eccentric rules and demands. If dystopia were to occur in a real-world environment, 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; they would lose their independence and relinquish their self-reliance due to the constraints on free will placed by governments.



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 through technology. One such portrayal is in Ray Bradbury's famous novel *Fahrenheit 451*, first published 1953. The similarities between humanity's current condition and Ray Bradbury's well-crafted, cold, detached characters 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 ICT 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, confidently hocking up everything from power plants to front door bells.

Like the child in the fairy tale "Little Red Riding Hood," innocently wandering through the forest, humanity erroneously believes that the "Wolf" is whoever he appears or claims to be. Just like Little Red Riding Hood, humanity is in danger of falling prey to a predator, with one significant difference: although disguised, Little Red Riding could see her predator, while humanity cannot, thanks to cyberstealth and the inherent anonymity provided by ICT. It is amazing how this fairy tale, created centuries ago, stands as a metaphor for the tactics of impersonation used in cyberbullying and online sexual predator stalking and "grooming." Unfortunately, the theme of a predator disguised as someone else is exactly what now occurs in cyberspace.

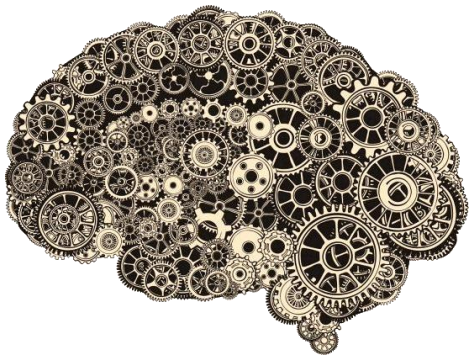
With the "cloak of anonymity" so conveniently provided by ICT, iPredators troll cyberspace with a distinct advantage: their ability to represent themselves in any way they choose. Furthermore, they can secretly stalk their prey by tracking the potential victim's path from an undetectable, safe distance. Not only can iPredators become anyone they choose to be, they can also become anyone their victim may subconsciously want them to be. Much of what was once considered private is now shared online, giving iPredators immense troves of highly sensitive psychological information to cull in search of vulnerable victims.

The repercussions of the unrestricted latitude of iPredators will be catastrophic for not only the individual, but for society. Before it is too late, society must re-examine the phenomenon of "social networking" via technology and must become educated in the dark psychology of ICT and the mighty potential for harm that lurks beneath its surface.

Invented by the novelist William Gibson in his 1982 short story "*Burning Chrome*," the term *cyberspace* describes the non-physical terrain created by ICT. 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 that mimics 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.

Although the benefits of information and communications technology far outweigh the detriments for society, humanity has been seduced by the illusory notion that more technology will always translate into a better quality of life.



The Illusion of Virtual Reality

Whereas virtual reality is positive and artificial, iPredators are both very real and potentially extremely dangerous. In all cases, iPredators exhibit active hostility to the victim's psychological welfare by injecting fear, embarrassment, and distress in their lives. Although the iPredator is the antithesis to the positive environment created by virtual reality, it is fair to assume that iPredators will include virtual reality in their future cyberstealth strategies as technology advances.

Given that 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 to know they exist both in the real world and in the abstract electronic universe. iPredator acts of theft, violence, abuse, cyber warfare, and cyberterrorism will grow into a global plague if not thwarted. Society cannot rely on governments to confront all groups of iPredators, because they are everywhere and live in our communities. Physical distance has lost all relevance. You can be cyber-attacked by some two continents away as easily as your neighbor.

The threat posed by iPredators is not confined to the abuse of specific individuals; it is a matter of national security; the evidence is clear that cyberwarfare will be to the 21st century what nuclear war was to the 20th: a ubiquitous threat of unimaginable catastrophe. Writing in the *New York Times* in June 2018, security expert David E. Sanger spoke of a "cyberarms race of historic but hidden proportions. In less than a decade," Sanger said,

> "the sophistication of cyberweapons has so improved that many of the attacks that once shocked us — like the denial-of-service attacks Iran mounted against Bank of America, JPMorgan Chase and other banks in 2012, or North Korea's hacking of Sony in 2014 — look like tiny skirmishes compared with the daily cyber-combat of today."

Presently, United States officials from the National Security Agency, Department of Homeland Security and the FBI must constantly be on alert for cybersecurity threats. The military currently relies on the United States Cyber Command 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 cyberterrorism, the global community must also concurrently prepare for both cyberterrorism and homeland iPredators.

Internationally, the legal steps taken toward collective enforcement of laws against cybercrime are so far woefully insufficient. The European Convention on Cybercrime currently requires signatories

> "to criminalize in their domestic law four classes: offences against confidentiality and data integrity (arts. 2–6), computer-related offences of forgery and fraud (arts. 7 and 8), computer-related offences of child pornography (art. 9), and offences related to copyright infringement (art. 10)."

However, "the essence of the Convention being cooperation, there is only an implicit obligation on each State party to prosecute the proscribed acts; there is no explicit obligation, absent prosecution, to extradite", rendering the law essentially toothless. Similarly, the U.S. "legacy act" known as the Stored Communications Act is considered by digital law experts

> "to be at once too vague in its definitions and obsolete in its distinctions … in the case law, significant uncertainty also remains because the Supreme Court has thus far refrained from clarifying if and when individuals have a reasonable expectation of privacy in digital communications."

As a result of this outmoded legal infrastructure, iPredators have lower probabilities of identification, legal ramifications, or injury. Prior to ICT, perpetrators had to be far more creative in their methods; now they can create counterfeit identities or manipulate others using embellished personas carefully tailored 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.

As described, iPredators use a tactical weapon this writer has termed "cyberstealth," offered by ICT, to taunt, troll, and stalk their prey. iPredators target online users, corporate entities, and organized groups that are oblivious, inexperienced, ill-informed, or unaware they are covertly being evaluated as potential targets. In nature, wild animals stalk and

measure their prey using stealth and tactical strategies, increasing their probability of success while decreasing the potential for injury. Similarly, iPredators use cyberstealth to stalk online users, increasing the probability of achieving their aims, while decreasing their potential of identification and punishment.

As this writer illustrates in his 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 dominant living organism on earth, we are also the apex of brutality upon ourselves and other living creatures. The prime targets sought by iPredators are ICT users who are not intellectually, psychologically, and technologically equipped to protect themselves. They lack ICT safety strategies and technology, heightened levels of awareness online, a healthy level of skepticism, comprehensive digital citizenship practices, and *C3* (cyber-safety, cybersecurity, and cyber-ethics) plans.

Computer science experts, sociologists, and psychologists tend to describe ICT and the internet as beneficial tools for humanity; the rise of social media networks has been built on a strain of utopianism that is naïve, at best, and willfully blind, at worst, to the negative effects of our all-encompassing technology. In creating the paradigm of the iPredator, this writer perceives this new dimension and the tools needed for access quite differently. The world wide web, telecommunications, digital technology, and mobile device technology are all highly beneficial tools and areas extremely helpful to society, but tools have many different purposes. When chosen for nefarious or malevolent reasons, ICT and the internet are tools that become weapons.

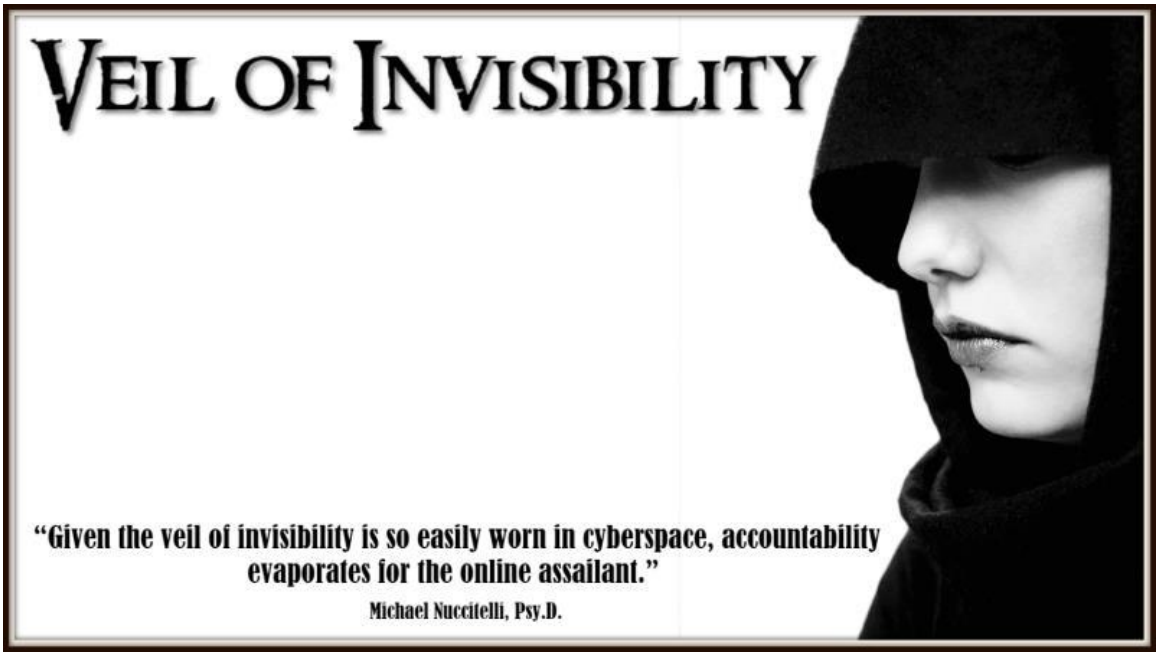
When weaponized, ICT can cause horrible and deadly consequences to both the citizens and communities of the countries they hail from. The future of cyberwarfare and cyberterrorism are both inevitable realities that have yet to cause massive harm to society. As this writer continues to research the growth, expansion, and underpinnings of iPredators, he has concluded cyber-warfare and cyberterrorism will become terms universally feared by humanity within the next two decades. Within five decades, industrialized nations will distribute most of their defense budgets to protecting their citizens from the potential devastation caused by iPredators.

Prior to ICT, 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 needed online and in cyberspace. 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 subdued as we exchange and verify information. ICT users try to find and confirm valid information while remaining completely isolated from

the source. The "veil of invisibility" that ICT and cyberspace offer humanity has many benefits, but the detriments can far outweigh the assistances for the vulnerable, unaware, or ignorant online user.

Given the veil of invisibility is easily worn in cyberspace, accountability evaporates for the online assailant.



"Veil of Invisibility" and Cyberspace

The child cyberbully tends to practice minimal online deception, given their need for recognition and peer acceptance. Depending on the cyberbully's strategy of taunting and harassment, their cyberstealth may range from nonexistent to cyberbullying by proxy. Cyberbullying by proxy occurs when a cyberbully coerces or encourages other online users, who do not know the target victim, to become an accomplice of the cyberbully and join in assaulting, taunting, or harassing the target child. The unfortunate result for the target child is they are deluged by hurtful and harassing information without knowing who or how many online users are attacking them.

At the advanced end of the cyberstealth continuum are online sexual predators, cybercriminals, and those looking to target online users motivated by violent or sadistic intent. Although most child sexual assaults take place offline by friends, family members, and young adults close in age to the target child, there still are thousands of online sexual predators.

As part of the human condition, humans tend to embellish their attributes, both offline and online, to present themselves as successful, popular, rich, attractive, and worldly. The

purpose of embellishing attributes is not to abuse or victimize the recipient, but to increase perceived worth. This form of "bragging" or "embellishing" has been a key aspect of interpersonal relationships since the beginning of humanity. Presenting oneself in the best possible light is not only restricted to humans but occurs among most 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, ICT users who brag about their attributes or material wealth are practicing the same behavior as the peacock, at a much cheaper cost.

Making sure we look good in that social networking site post is a part of human nature, albeit one that is distorted by the ubiquity of social media. It is only when the images and words produced are specifically intended to deceive, with the intention of causing harm, that the behavior crosses the line into the realm of the iPredator. Online deception needs the motivation to harm other ICT users to meet criteria for iPredator. ICT can paralyze humanity's innate evolved instincts for "survival of the fittest" and cause many to lose sight of being skeptical and wary of people met in cyberspace. For this reason, it is always vital to be wary of what others show online and the modus operandi behind their statements.

Although federal, state, and local officials work diligently to combat iPredators, their endeavors are minimal given the size of the iPredator contingent and their international cohorts. iPredators have the luxury of trolling for victims at a leisurely pace without fear of punishment. Unassuming ICT users are easily lulled into complacency and let their digital defenses down because they are either ignorant of iPredator cyberstealth practices, seeking social acceptance by someone they think will "like them," or engaged in high-risk online behaviors, all of which increase their probability of being targeted. In addition, many iPredator victims score very low on a psychological measure called *thoughtfully reflective decision-making*, or TRDM. Writing in the *Journal of Research in Crime and Delinquency*, criminal psychologists Eric R. Louderback and Olena Antonoccio argue that

> "individuals with low levels of TRDM may be more likely to be victims of computer-focused cybercrime. This is because they are less likely to engage in thoughtful cognitive decision-making processes when taking steps to protect their computers against potential victimization. Specifically, they may not collect all relevant information regarding what can be done to secure their electronic devices (e.g., utilization of antivirus programs and regular computer updates) and may neglect to consider all possible options for doing so (e.g., consulting computer experts and seeking out educational resources on computer security topics)."

A simpler model for assessing vulnerability to iPredators is the abbreviation D4, which stands for *distracted, distressed, discouraged*, or *dysfunctional*. Minimal research on psychological functioning and online victimization suggests ICT users' mental states will hinder their ability to practice responsible and safe ICT activities. Fueled by anger, depression, greed, narcissism, and psychopathy, many iPredators revel in their ICT

anonymity. Many also become grandiose from their criminal and abusive triumphs and feel galvanized knowing they can freely troll for potential victims, 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.

With little fear of apprehension, iPredators participate in the creative design and focused purpose in their line of attack. As part of the human condition, all humans experience exhilaration and satisfaction when they are triumphant. For iPredators, they experience the same states of exuberance, but at the expense of their victims. The more malevolent the iPredators' endeavors are, the greater sense of accomplishment they feel.

Given the obvious benefits ICT offers, time spent interacting online will increasingly become commonplace for all humanity; the dimension of cyberspace is unchartered 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 their minds the serious potential for their identification, apprehension, and prosecution when they engage in nefarious or malevolent online activities. The threat becomes especially potent when we consider how exponentially mobile computing and internet use continues to grow; a world with every citizen walking around with unsecured mobile devices is "iPredator Utopia."

The 5PV Model

iPredator, iPrey, iPrevention, iPreservation, iVictim

5PV is a five-factor theoretic model used to conceptualize digital abuser/victim dynamics and all social interactions between people who use ICT and the internet. These online users are segmented into three distinct groups categorized by their ICT intent, actions, and motivations. The first group is users who access and interact with other ICT users for benevolent or purely social reasons. They use ICT 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 ICT 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 look to harm others.

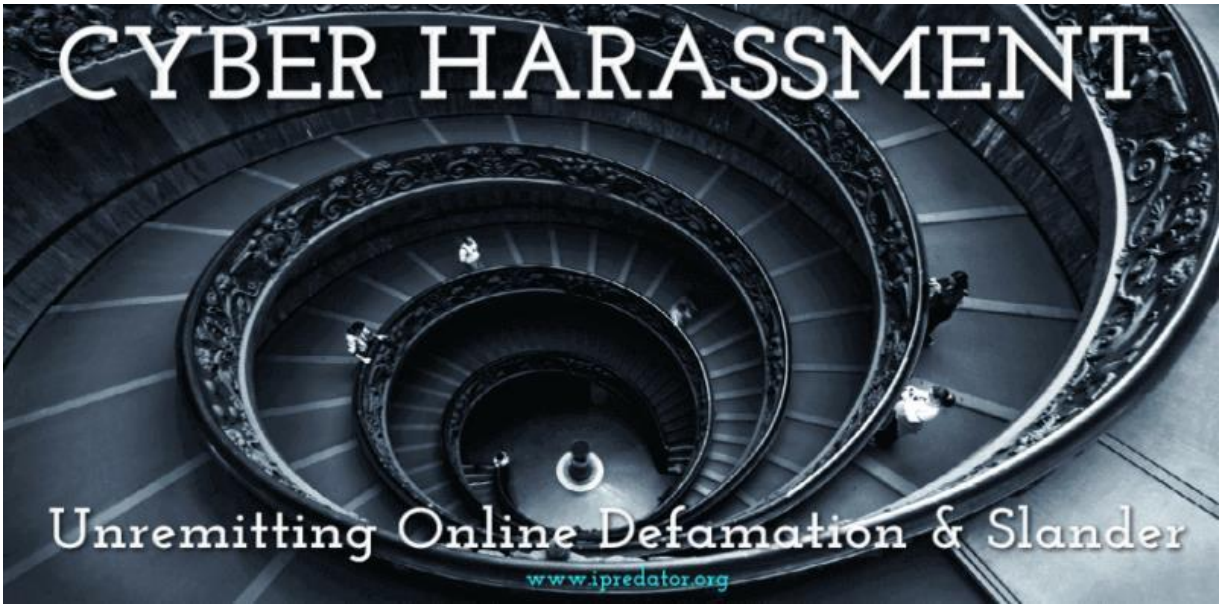
The third group consists of those who may occasionally stray into abusive or deceitful practices online, but who do not meet the criteria above for being a true iPredator, largely because their psychopathology is not advanced enough to endow them with the cunning and delayed gratification that are the hallmarks of the true iPredator. It is nearly impossible to estimate how many ICT users there are and how they divide into these three groups; as

ICT and information security become more advanced fields, the need for metrics and statistical data-gathering will become ever more acute.

The five terms of 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 ICT, cyberspace, and 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 the offender and victim interact. This environment, which works to the advantage of the iPredator, is the *Geosocial Universe*. It is in this realm of cyberspace that iPredators can create a persona judged effective in their tactical strategy to achieve success in stalking.

For example, a forty-year-old man can create an online social profile tailored exactly to how he feels it 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, and then interact with his teen targets as someone close to their age, gender, and stage in life, with all the same "likes" and "dislikes" often discussed and rated online. Meanwhile, his potential targets innocently interact with him, completely ignorant of his identity. This is only one example of the hundreds of ways iPredators use cyberstealth in cyberspace.

Many iPredators evaluate their target quarry by first assessing if they are exercising personal security, harm reduction, or victim prevention measures. The concept of *iPrevention* describes an ICT user sustained practice of internet safety, cybersecurity, and self-awareness of how they are perceived both offline and online.



iPrevention is Key to Cyber Safety

iPrevention is a strategy, practice, and conscious and 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 is in close geographic proximity to their target, they will use all available observations to estimate the success rate of their cyber-attack. As ICT will always advance, iPrevention as well must be a proactive and progressive activity. This is not to say that iPrevention needs advanced training in ICT, but a sustained effort to learn and evolve given its rapid expansion.

What is needed is a willingness to exercise diligent awareness, accepting as given 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 to be 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 ICT, by practicing consistent and effective iPrevention.

Everyone learns, practices, and persistently works on developing their skills, and this applies equally to iPrevention. Equally important in iPrevention is what the ICT user does if they are cyberattacked. Given that the laws of probability say all ICT users will be confronted with some form of iPredator attack in their life, the steps one takes as soon as the cyberattack is started helps to reduce the negative consequences the attack intends to achieve. When instituting iPrevention, the ICT user is exhibiting *iPreservation.*

iPreservation is defined as an innate state of self-survival that manifests in an online user's ICT 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, before it develops much more.

iPreservation and ODDOR

This simple concept of *Offline Distress Dictates Online Response*, or ODDOR, postulates that both a child and adult's response to their offline environment is directly correlated to how they behave online. ODDOR is thus a basic formula for all cyber protection and ICT safety initiatives by online users, based on 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. ODDOR is a phenomenon new to information age human consciousness.

iPreservation is an internal experience that signals the online user to behave and act so when online or engaged in ICT usage. Although self-preservation is ingrained in all living organisms, some ICT users lose this instinct in cyberspace. Just as the anonymity of

cyberspace allows some ICT users to act and behave uncharacteristically, the same phenomenon occurs in the realm of self-preservation. Because there is not another person or entity in front of them when online, some ICT 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 ICT user may not be online alone, 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 ICT and online safety skills also include awareness of how offline behavior and lifestyle can change online behavior. Far too many adults and parents are not aware 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 concept of iPredator, the one theme emphasized throughout his entire philosophical framework is as follows:

Information and Communications Technology (ICT), social media, and cyberspace itself has the uncanny ability to tap into our perceptual world and distort our interpretations of oneself and others. For those who experience gratitude, it helps the human condition and community. For those who suffer wrath, anguish, or ingratitude? Condemnation of self and society becomes the weapon.

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 who have been highly

stressed offline are profiles the iPredator looks to target. Depending on the advanced IVI (iPredator Victim Intuition) of the iPredator, an online user's ODDOR can be quickly recognized by an iPredator.

As said, 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 seen in online users who recognize that 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 humanity in the digital world, given that iPredators are protected by cyberstealth, guided by conquest and domination, and growing in numbers as ICT evolves and spreads. iPreservation is also defined as an instinctual motivation to institute a set of behavioral goals 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 need to preserve their safety and engage in the tactics and strategies to ensure their identity is not divulged.

The ideal target for an iPredator consists of an ICT user who does not take the necessary steps needed to reduce their probability of becoming a mark. High-probability ICT user targets tend to practice denial, viewing themselves as too technologically advanced to fall within the purview of an iPredator. When one or more of these elements are perceived by ICT users, they are in the arena of an iPredator, whose antisocial pursuits are fueled by their distorted beliefs of self-preservation, narcissism, and the need to dominate and control. Many of these miscreants believe they must victimize others to thrive and even sometimes to survive, to feel socially accepted, and often, to gain a sense of accomplishment, right, or vindication.

Their motivation to harm others is not always restrained by guilt or remorse, because they perceive their actions towards a target or victim are deserved: the online user should have expected it given their attitude, actions, or ignorance. Perceiving their actions in this way allows iPredators to justify the purpose of their malevolent and nefarious behaviors and to harm others without feeling remorse. Given that the concept of iPredator includes all ICT users who try to taunt, victimize, or abuse others using ICT, the easiest way to define the cornucopia of perpetrators and their core concepts is as lacking a 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 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 inspire people to help others, are central to a person's

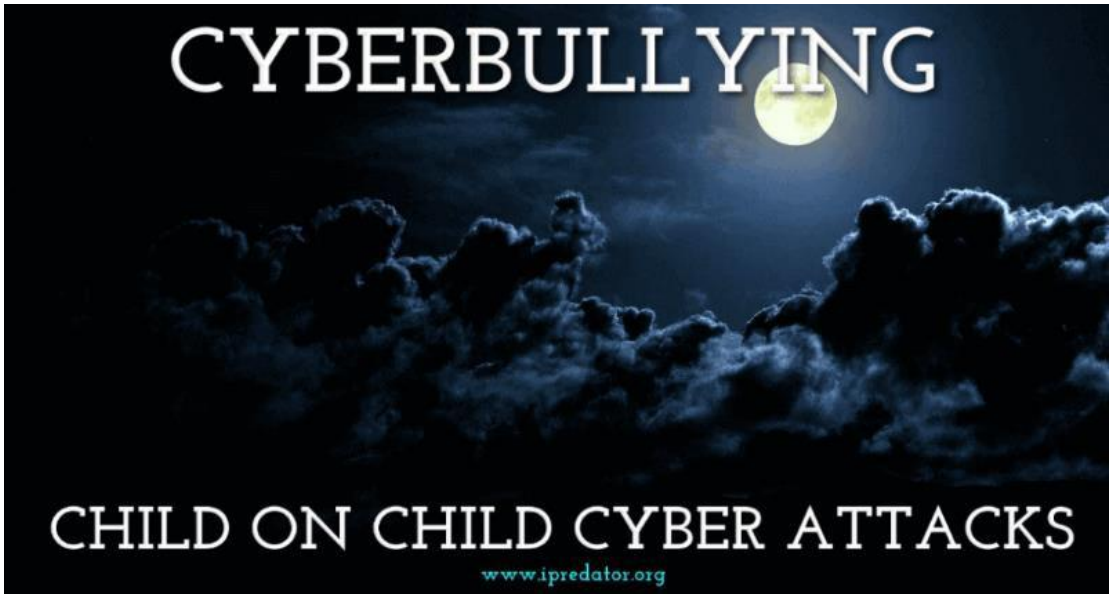
sense of well-being, stable mental health, and functional adaptability. For Adler, there will always be some whom society judges as "failures" because

> "they do not meet the expectations of socially interested people. Their deviations appear when they meet any problem of life which demands more social interest in its solution than they have acquired. Not prepared, they believe or are sure that they are blocked. But life with its inherent and vulnerable structure of striving for a successful achievement does not permit a standstill. Either the shock results prevail, or a certain degree of continuing activity gives rise to an antisocial solution."

From this thesis, Adler strongly believed people with low social interest were discouraged, angry, and enveloped by a sense of inferiority, or what he termed an inferiority complex. The advent of ICT has provided myriad avenues for the actuation of these "antisocial solutions"; indeed, Adler noted that "the unsocial or anti-social individual or group is always more restless and alert in planning attacks." His theory of social interest conceived a century ago, certainly defines what appears to be an iPredator's proclivity to behave in an abusive, hostile, aggressive, criminal, or deviant manner.

As cost decreases with ICT, 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 that iPredators do not stalk for survival, food, procreation, or territory. They stalk their quarry for deviant sexual needs, distorted sociopathic endeavors, criminal intentions, immature developmental needs for acceptance, or psychological and psychiatric issues. iPredators tend to be male, but the ranks of female iPredators are steadily growing at a rapid rate as ICT becomes more commonplace.

The motivation for iPreservation is not based on fear of iPredators, but rather on the awareness they exist.



Cyber-Attack Prevention

The entire population of online users in the 5PV model of criminal, deviant, and harmful interaction, called iPrey, stands for all the potential targets in an iPredator's reservoir of choices. Everyone who interacts with ICT falls within this broad group. Just as a massive herd of wildebeest are all viewed as fair game to a pride of lions, so too are all online users' potential targets for iPredators. Everyone who interacts with ICT falls within this group. iPrey can be a low, medium, or high probability target for iPredators. Low probability targets are ICT users who are consciously aware there are malevolent people online who will try 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 statement is not to say that children, females, or senior citizens cannot practice ICT and internet safety or insulate themselves from victimization, but certain factors outside of their control, such as age and gender, place them in the preferred target populations of an iPredator.

High probability targets, or iPrey, are ICT users who do not practice ICT and online safety for assorted reasons. These reasons include ignorance of internet safety and security, thinking they are irrelevant, simply not caring, and 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 ICT user either for personal or professional use. Even when a person stays a proactive online user, engaged in a healthy offline lifestyle, skilled at practicing internet safety and diligent in their practices, it remains still especially 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.

The most vulnerable targets for both the animal and insect predator and iPredators consist of the young, the old, the feeble or wounded. Given that the clear majority of iPredators tend to be males, they often target females due to their distorted belief that females are weaker or less clever. This rule does not apply to cyberbullies, as these segments of iPredators are primarily the same gender. The role of males being the predominant online perpetrators is quickly changing as ICT becomes more relevant to societal communications. Although males continue to make up the larger group of ICT offender, the rate of females becoming iPredators steadily increases.

Ignorance, discouragement, psychological imbalance, lack of skepticism, isolative tendencies, and curiosity are but a few traits an iPredator looks for in hunting for an

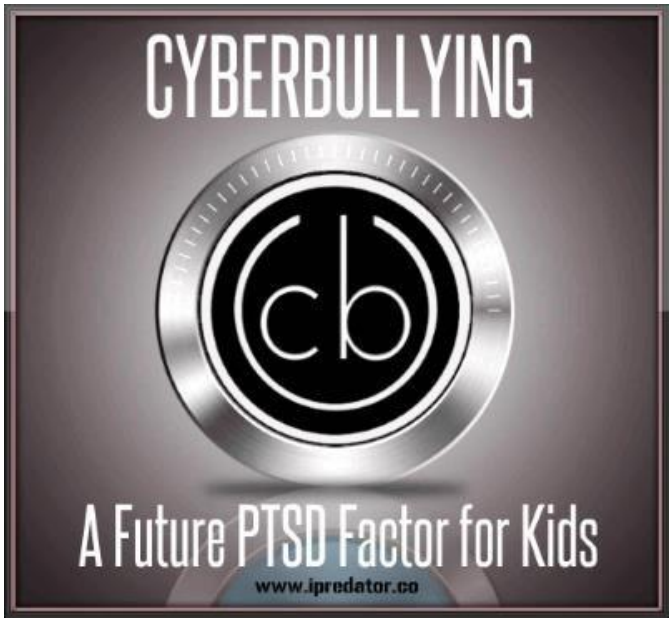
iVictim. In addition to being adept at practicing cyberstealth, iPredators are trained at sensing the qualities that they think helpful to start the hunt.

Cyberspace can be a classroom, insane asylum, dance floor or lethal weapon. It is your choice what metaphor you choose.

It is undoubtedly so that ICT will bring many wondrous things to humanity. From the large of Cosmology to the small of Quantum Mechanics, and to the personal of Physiology & Psychology. All aspects of science and the human condition profits. We are living at the beginning of a period in history called the Information Age. Civilization will evolve in ways we cannot imagine.

If humanity is not judicious and ignorant of the dark side of cyberspace; cybercriminals, the ideologically extreme and unscrupulous politicians adorn the headlines. Children humiliate and torment other children devoid of accountability. Society increasingly disconnects, and the discouraged psychologically isolates. For some, their online identities become more valuable than their offline identities. The perceptually distorted accepts cyberspace as real and factual, despite it being an artificial digital environment.

It is imperative for educational systems to make internet safety and digital citizenship compulsory academic requirements. Adults must learn about the consciousness altering effects of ICT and how offline distress dictates an online response. Included in their ministries, spiritual leaders must stress patience and forgiveness as integral when cyber-attacked. Academic institutions, governments, the legal system, and healthcare need to understand how ICT affects intrapersonal and interpersonal dynamics. If we do not, iPredators will become the bane of our existence.



iPredator Typologies

Cyberbullying

Cyberbullying is threatening, or disparaging information directed at a target child delivered through Information and Communications Technology (ICT). Like traditional bullying, cyberbullying is harmful, repeated, and hostile behavior intended to taunt, embarrass, deprecate & defame a targeted child. Dissimilar to traditional bullying is cyberbullying includes a phenomenon called "Cyberbullying by proxy". Cyberbullying by proxy is when a cyberbully encourages or persuades other ICT users to engage in deprecating and harassing a target child.

Cyberbullies are usually motivated by a need for peer acceptance and/or power and control. A small percentage of cyberbullies engage in these maladaptive behaviors out of ignorance of the distress they cause a target child. The most malevolent form of cyberbully, the Narcissistic Cyberbully, feels minimal remorse for the harm they inflict upon their victim. It has been speculated that children view the real world and the online or virtual world as part of a seamless continuum.

Cyberstalking

Cyberstalking is the use of ICT to stalk, control, manipulate or habitually threaten a child, adult, business, or group. Cyberstalking is both a tactic used by an online assailant and typology of iPredator. Cyberstalking tactics include false accusations, threats of physical harm, habitual monitoring, surveillance, implied threats, identity theft and the gathering of information for manipulation and control of the target.

To meet the criteria of cyberstalking, 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, dis-information dissemination, and environmental damage to the target's reputation, credibility, or financial status if the target does not acquiesce to the cyberstalker's demands.

Cybercrime

Cybercrime is a criminal activity using ICT as tools to target victims, groups, or businesses. All forms of cybercrime involve both ICT and a target. Cybercrime is segmented into two distinct categories involving the focus of the cybercriminal activities. These activities are focalized on the technology of ICT either to achieve the cybercriminal's aims for personal and financial gain, or for widespread use against business or governments.

When the individual is the main target of cybercrime, ICT is the tool rather than the target, and the crimes are often the same as those that have existed for centuries in offline societies. Cybercriminals use technological tools to increase their potential pool of victims and make them difficult to find and apprehend. The most common types of cybercrime are identity theft, hacking, online swindles, fraud, computer system attacks, illegal online content, prohibited online content, and digital piracy.

Cyber Harassment

Cyber harassment is the use of ICT to torment, control, manipulate, or habitually disparage a child, adult, business, or group without a direct or implied threat of physical harm. Unlike physical harassment, which involves face-to-face contact, cyber harassment relies on ICT; the cyber harasser's primary goal subsists in trying to exert power and control over the targeted victim.

When minors are involved, cyberbullying is the term describing cyber harassment; when direct or implied physical harm to the targeted victim becomes involved, cyber harassment becomes cyberstalking. Another similar term often used to define cyber harassment, but slightly different in perpetrator modus operandi, is "Internet Troll."

Cyberterrorism

Cyberterrorism has multiple definitions and applies to a variety of cyber-attack intricacies that may involve one online perpetrator or many. As a typology of iPredator, cyberterrorism is defined as the cognitive, affective, behavioral, and motivational factors of terrorist groups or their agents who use ICT to impair, harm or destroy non-combatant targets. Cyberterrorism is different from activism, hacktivism, and cybercrime in that the primary purpose of a cyberterrorist attack is to cause physical violence or extreme financial harm.

Per the US Commission of Critical Infrastructure Protection, cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. More generally, cyberterrorism tries to interrupt, destroy, or exploit another group or nation's ICT vulnerabilities to adversely affect their critical infrastructure.

Online Predators and Online Child Pornography

Online Predators have a variety of different terms used to describe the same patterns and motivations for their abuse. Historically, those who are not familiar with the profiles of sexual predators, pedophiles, and child molesters tend to view them as being easily found and incompetent. Not only are most sexual predators their victim's neighbor, relative, or mentor, but the "veil of anonymity" in cyberspace makes correct perpetrator identification a daunting task.

Online Predators are defined as adult online users who look to exploit vulnerable children or adolescents for sexual or other abusive purposes. Online Predators are sexual predators who use ICT and social media to find, target, and victimize minors. Although online sexual predation transpires between adult online users, the underage minor child remains the primary target. It is important to note that the myths of Online Predators do not often match up with the reality. According to *American Psychologist,* the widely held concept of

> "online predators who prey on naive children using trickery and violence is largely inaccurate. Internet sex crimes involving adults and juveniles more often fit a model of statutory rape—adult offenders who meet, develop relationships with, and openly seduce underage teenagers—than a model of forcible sexual assault or pedophilic child molesting."

Online child pornography is defined as the production, consumption, and distribution of sexual content involving minors. Although it qualifies as an iPredator typology, it also falls within the online child predator genre. To be more specific, online child pornography includes online users who are sexually aroused or financially motivated by online sexual content involving minors. Consumers and distributors of online child pornography are not all sexually aroused by the content; some are motivated by the financial rewards to be gained.

Internet Trolls

An internet troll is a colloquial expression used to define an online user who uses ICT to provoke, defame, anger, tease, flame, or incite other online users. Often, the internet troll does not know the target recipient of their vitriolic statements and behaviors. Internet trolls regularly appear in all forms of online mediums ranging from online video gaming

gatherings to chatroom and forum discussions, and, especially pertinent to the evolving landscape, on social media channels such as Twitter, YouTube, Instagram, and Facebook.

The motivations for an internet troll's provocative behaviors are many. Despite the variations in modus operandi, most trolls are seeking attention, recognition, stimulation, pseudo-notoriety, and retribution for some unknown perceived injustice. Although there is no current hard evidence or clinical research confirming the psychology of the internet troll, it is believed that the "veil of anonymity" afforded to every online user inspires some to engage in egregious behaviors.

The dark side of cyberspace is a metaphor and conceptual framework defining a virtual environmental realm that includes all criminal, deviant, deceptive, harmful, and malevolent activities in the abstract universe of cyberspace. Whereas iPredator is a criminal, deviant, and disturbed typology concept, the dark side of cyberspace also includes legal and illegal online activities, as well as destructive and self-destructive online behaviors.

iPredator Relevant Concepts

Dark Psychology (2006)

Dark Psychology is the study of the human condition as it relates to the psychological nature of people to prey upon others. All of humanity has this potential to victimize other humans and living creatures. While many restrain or sublimate this tendency, some act upon these impulses. Dark Psychology looks to understand those thoughts, feelings, and beliefs that lead to human predatory behavior. Dark Psychology assumes that this production is purposive and has some rational, goal-oriented motivation 99.99% of the time. The remaining .01% is the brutal victimization of others without purposive intent as defined by criminology, evolutionary science, or religious dogma.

Dark Psychology posits there are people who commit these same acts and do so not for power, money, sex, retribution, or any other known purpose. They commit horrid acts without a goal. Simplified, their ends do not justify their means. There are people who violate and injure others for the sake of doing so. Within all of us is this potential. This potential to harm others without cause, explanation, or purpose is the area explored by Dark Psychology, which assumes this dark potential is incredibly complex and even more difficult to define.

iPredator Bridge

iPredator Bridge is a theoretical branch of the iPredator paradigm that models the psychological, perceptual, and behavioral trajectory of people who use ICT to harm others out of self-righteousness, moral turpitude, religious/political/philosophical convictions, and pro-social perceptual distortions. Not driven by criminal, malevolent, or deviant endeavors, iPredator Bridge looks to define why some people approach the nefarious and malevolent realm of iPredator, decide to go ahead, and then continue along a trajectory where their cognitive, affective, behavioral, and perceptual actions harm others or societies.

Like the iPredator, individuals on the iPredator Bridge spectrum are motivated by personal convictions, greed, power, control, narcissism, or psychopathology. Unlike the iPredator, they have yet to fully engage in criminal deviant activities using ICT, or to use complex perceptual distortions to confirm the harm they cause. iPredator Bridge investigates why some people approach this malevolent realm and either continue in their maladaptive trajectory or cease and desist.

Offline Distress Dictates Online Response (ODDOR)

Offline Distress Dictates Online Response (ODDOR) is a sub-tenet of iPredator, which posits that offline psychological functioning directly influences one's online interactions. Whether someone is an online assailant, cyber-attack target or both, ODDOR does not discriminate. ODDOR postulates that temporary and long-standing psychological states can significantly taint an online user's behaviors and interpretations. Perceptually isolated, ignorance of the existence of ODDOR and experiencing atypical affective and cognitive states increases the probability of being targeted by an online assailant.

In addition to being at a greater risk of being cyber attacked, ODDOR influences an online user to partake in destructive and self-destructive online activities. If a person is self-aware and healthy, their levels of ODDOR are less likely to become problematic. Just as self-awareness acts as a buffer between mental health and dysfunction, the same holds true for ODDOR.

Troll Triad

Troll Triad is a cyber-psychopathology and profiling concept that introduces a three-pronged archetypal model defining groups of online users who engage in defamation of character, slander, and libel. Troll Triad is not just a facetious term describing groups of malevolent online users who use ICT to defame, manipulate, curry favor, and seek support from other like-minded online users, but a conceptual framework and template describing how groups of successful iPredators are partitioned into three archetypal segments. This troika includes the Cerebral, the Provocateur, and the Crier.

The Cerebral is the user who relies on a false sense of superior intellect to demean his targets; he often uses a kind of parody of logical argument when attacking his perceived opponent. The Provocateur's behavior is marked by deliberately outrageous statements or insults that are meant to diminish and belittle. And the Crier's archetype is dominated by a sense of tragic outrage, typical of those who feel that some element(s) of society has wronged them. When these three elements mix correctly, the Troll Triad becomes a masterpiece of human predation alchemy. Being a disciple of Carl Jung and Alfred Adler, I strongly subscribe to Jung's theory of archetypes and Adler's theory of social interest. Using their concepts as guidelines, Troll Triad is a concept relevant to the information age.

Predatory Trolls

Predatory trolls are a new breed of internet troll, evolved from the classic troll. They are online users who choose online targets both randomly and intentionally. Just like classic trolls, predatory trolls can be ex-work associates, ex-partners, and loved ones as easily as they can unknown online users. Predatory trolls may target others alone, but increasingly work in groups (see Troll Triad). Like all trolls, Predatory trolls are driven by needs for power, recognition, peer acceptance, and control.

Predatory trolls differ from classic trolls in that their primary goal is to destroy an online user's reputation, online presence, and trustworthiness. With the advancement of ICT, predatory trolls may be employed by groups and governments in covert operations to destroy a target's reputation. Predatory trolls look to destroy their target's reputation and the reputation of their family members, children, careers and loved ones.

Online Psychopathy (iPredopathy)

Online Psychopathy, or iPredopathy, is an information age criminology and human consciousness concept that replaces pre-information age profiles of sociopathy and psychopathy. iPredopathy is an advanced stage characterological disorder describing any adolescent to adult male or female who skillfully uses ICT to troll, manipulate, and control their human targets. Driven by grandiosity, sexual perversion, or perceptual distortion, iPredopaths experience no remorse or shame for the harm they cause others. Like iPredators, many iPredopaths do not break the law and live unscathed by law enforcement, fraternal organizations, religious institutions, and the legal system.

Using cyberspace (including the so-called Dark Net) and electronic devices, Online Psychopaths (iPredopaths) design and implement their criminal, deviant, violent, deceptive, and cyberstalking tactics. Their human quarries are unsuspecting, vulnerable, submissive, and internet safety-ignorant children, older adults, unprepared businesses, and psychologically distressed adults.

Phantasist

A Phantasist is an online user who obsessively prioritizes and refines their online profile, avatar, or persona while engaging in malevolent or nefarious activities. In most cases, they use the online persona to hide their identity and exploit or intimidate others. The Phantasist has difficulty differentiating their true self from their online identity, which places them on the far end of the Reality-Virtuality Continuum.

Although probable, a Phantasist does not have to suffer from a mental illness, personality disorder, or medical condition. For unknown reasons, the Phantasist increasingly becomes absorbed by their online identity. Enveloped by their online identity, they enter what is called the "Aspect," a psychological and perceptual realm whereby their offline life becomes

indistinguishable from their online life. Age of onset, the frequency of Aspect states, and time spent online determine the severity of the Phantasist.

Information Age Education (IAE)

Information Age Education (IAE) is a cyber-attack prevention paradigm offering a resolution to reducing the negative consequences of living in the information age. Information and Communications Technology presents positive and negative influences upon humanity, in which the negative aspects grow at a feverish pace, as we have seen. IAE prioritizes prevention education, non-denominational family values, and humility as solutions to connecting the disconnected, educating the ignorant, and conquering the corrupt.

IAE assumes that, along with the plethora of gifts and benefits information technology offers society, the dark side of cyberspace has ensnared an ever-growing number of the online citizenry. IAE suggests that people of all ages are migrating towards a state of disconnectedness, shying away from tangible interpersonal relationships, family values, the practice of humility, and basic kindness. IAE asserts that the only way to thwart the disintegration of connectedness is by awareness and cyber-attack prevention education.

Information Age Wellness (IAW)

Information Age Wellness (IAW) is the practice and study of how ICT influences people's physical, psychological, perceptual, and spiritual well-being. By incorporating safe and productive knowledge and practices, citizens and their loved ones in this information age are both safer from cyber-attacks and better able to focus on holistic wellness. IAW incorporates mind, body, spirit, and technology for those seeking a healthy lifestyle.

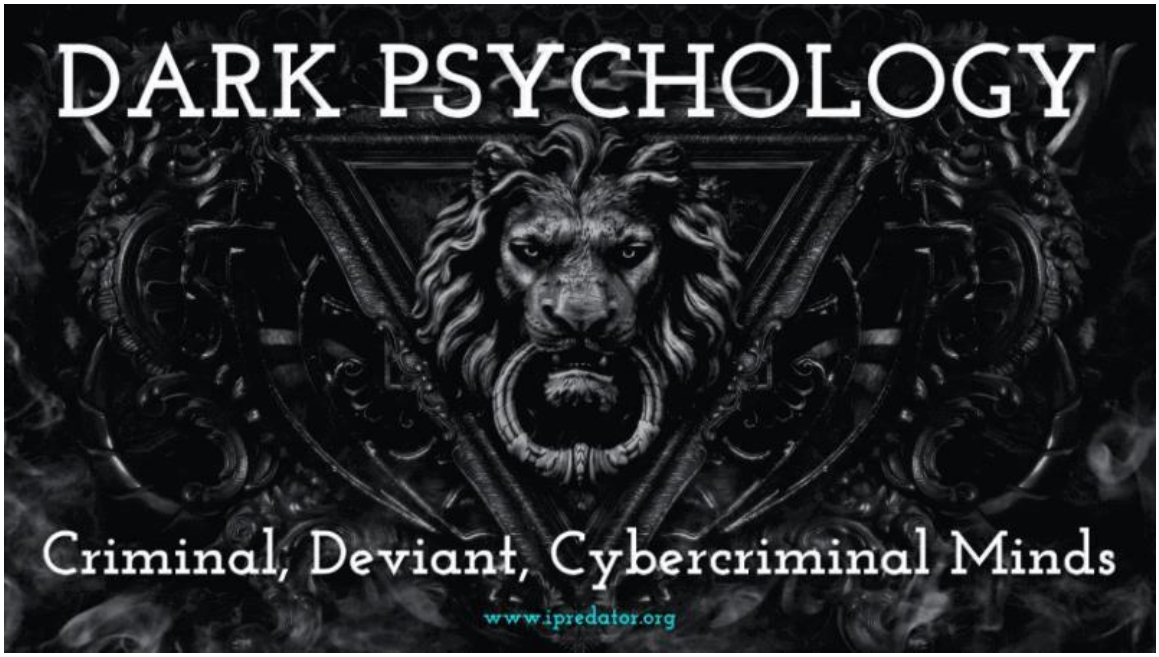
IAW combines internet safety, spirituality, integrative medicine, and health psychology while recognizing the growth of information technology and people's growing dependence upon it. IAW should not be confused with online healthcare, telemedicine, e-health, or any other medically themed field that works with ICT. Information Age Wellness is a conceptual framework that includes physical health, adaptive psychological functioning, spiritual health, and well-being in relationship to technology.

Information Age Forensics (IAF)

Information Age Forensics (IAF) is the science and technology of investigating the typologies, motivations, tactics, and psychopathology of iPredators. IAF examines the iPredator typologies of cyberstalking, cyber harassment, internet trolling, cybercrime, online sexual predation, cyberterrorism, and habitual online deception. Vital to full comprehension of IAF is considering valid the premise of iPredators being variants of the classical criminal, deviant, and aggressor. Information technology and cyberspace are not

simply tools used by information age aggressors (iPredators). They are a fundamental part of this new generation looking to harm, victimize, control, or dominate their chosen victims.

One of the demands of the iPredator paradigm is emphasizing how ICT is not a new tool for old crimes; it is an essential element of these crimes' ontological status, profoundly imbricated in the digital-psychological continuum. It is an error to think of ICT as simply a new set of tools for an old set of pathologies. Thus, Information Age Forensics (IAF) integrates the fields of Criminal, Cybercriminal, Abnormal and Developmental Psychology with iPredator and Digital Forensics Investigation.



Internet Addiction

Internet Addiction, also known as Internet Abuse, Internet Dependence, and Internet Use Gaming Disorder, is an umbrella concept defining a child or adult's compulsive and progressive abuse of the internet and electronic devices designed to obtain, exchange, or send information. Although the internet is the predominant arena in which Internet Abuse takes place, electronic devices and communication channels that are not internet enabled are included as well. Internet Abuse causes dysfunctional cognitive, affective, behavioral, and perceptual intrapersonal consequences, accompanied by employment, academic, familial, peer, and intimate partner interpersonal consequences.

On a continuum of severity, ranging from absent to mild, cessation of the internet or electronic device usage causes withdrawal symptomology, psychological and physiological, combined with perceptual tolerance. Also, on a continuum of severity, internet abusive online users engage in criminal, deviant, or deceptive online activities ranging from absent

to severe. The chronic and more debilitating condition, Internet Dependence, is potentially severe and self-destructive.

Cyberspace is an Extension of Human Consciousness (CEHC)

CEHC is a theoretical concept positing that ICT is gradually becoming, or already is in a rudimentary form, an extension of human consciousness and subjective processing. It is postulated that the digital universe is an abstract and artificial realm, which is evolving into an exact replica of the human brain. Neuronal connections and digital networks appear incredibly similar. Place an image of the internet and an image of the brain's neuronal connections side-by-side and they look the same.

It is easy to accurately conclude that a vast number of thinking human beings have created technology. Under this premise, it is not a leap of faith to assume that a legion of brains, in working on technological advancements, is creating a replica of itself: an inorganic facsimile of the most complex organic machine, the brain. The closer our collective brain gets to creating a copy of itself, the more human consciousness will view cyberspace as an attractive and seductive realm.

The brain and the unconscious are designed to have self-preservation as the primary goal. Since the physical body is finite, a day will come when human consciousness will be capable of transferring aspects of itself to the vast ocean of cyberspace. CEHC is not artificial intelligence, but the future destination of the extended mind & human consciousness within a digital framework. Advancements in nanotechnology, quantum mechanics and artificial intelligence will significantly change the human condition and the fields of Criminology & Psychology.

When one trillion plus neuronal connections connect to the quadrillions of digital connections in cyberspace, the dance between organic and inorganic networks begins.

Michael Nuccitelli, Psy.D.

Michael Nuccitelli, Psy.D. is a NYS licensed psychologist and cyber criminology consultant. He completed his doctoral degree in clinical psychology from Adler University in 1994. In 2010, Dr. Nuccitelli authored the dark side of cyberspace concept known as "iPredator." In November 2011, he established iPredator Inc., offering educational, investigative, and advisory services involving online perpetrators, cyber-attack targets, and the dark side of cyberspace. Dr. Nuccitelli has worked in the mental health field over the last thirty-plus years and he has volunteered his time helping cyber-attacked victims since 2010. His goal is to reduce victimization, theft, and disparagement from iPredators.

In addition to aiding citizens & disseminating educational content, Dr. Nuccitelli's mission is to start a sustained national educational and awareness internet safety campaign with the help of private, state, and federal agencies. He is always available, at no cost, to interact with online users, professionals, and the media. To invite Dr. Nuccitelli to conduct training, media engagements, educational services, or consultation, please call him at (347) 871-2416 or via email at drnucc@ipredator.org.

"Comfort the Victims, Educate the Ignorant, Conquer the Corrupt"

Sources Cited

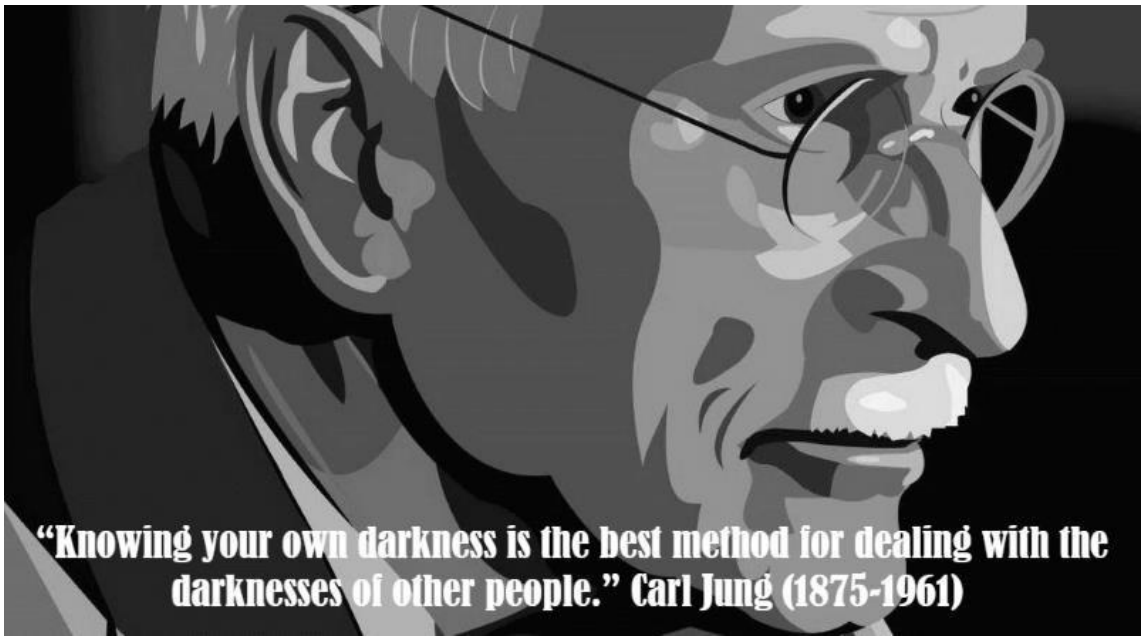
"those in abusive relationships …" Reyns, Bradford, et al. 2018. "Opportunity and Self-Control." *American Journal of Criminal Justice*: 1-20.

"the sophistication of cyberweapons …" Sanger, David E., 2018. "Cyberweapons and the New World Order." *New York Times*, June 5, 2018.

"to criminalize in their domestic laws …" European Convention on Cybercrime. Council of Europe, European Treaty Series no. 185. Accessed at http://www.europarl.europa.eu/portal/en

"to be at once too vague …" Renda, Andrea, 2015. "Cloud Privacy Law," in *Regulating the Cloud*, edited by Christopher S. Yoo (Cambridge: MIT Press).

"individuals with low levels …" Louderback, Eric, and Olena Antonaccio, 2017. "Exploring Cognitive Decision-Making Processes." *Journal of Research in Crime and Delinquency* 54 (5).

"they do not meet the expectations …" Adler, Alfred, 1937. "Psychiatric Aspects." *American Journal of Sociology* 42 (6): 776 ff.

"online predators who prey …" Wolak, Janis, David Finkelhor, Kimberly J. Mitchell, and Michele L. Ybarra. 2008. "Online 'Predators' and Their Victims: Myths, Realities, and Implications for Prevention Treatment." *American Psychologist* 63 (2): 111–28.