iPredator Bridge Warning Signs Checklist

IBWSC

MICHAEL NUCCITELLI PSY.D., C.F.C.

IPREDATOR BRIDGE WARNING SIGNS CHECKLIST

(IBWSC)



iPredator Bridge Warning Signs Checklist (IBWSC): Based on the iPredator Bridge construct, the iPredator Bridge Warning Signs Checklist (IBWSC) is a 50-item checklist designed to investigate if a loved one, colleague or peer is participating in or close to participating in harmful online and/or ICT activities towards others. Multiple affirmative responses to IBWSC statements suggests the person being queried exhibits patterned and/or observable behavioral patterns indicating they may be engaged in iPredator activities. The IBWSC focuses on confirmed behavioral observations and not upon personal convictions and/or philosophical reasons for harming others online or using ICT.

The IBWSC assumes there are both people engaged in nefarious and malevolent activities and those engaged in harming others driven by distorted beliefs they are doing so for righteous and/or morally supported reasons. The common thread identical in both segments is the victims they target suffer from their attacks.

The IBWSC has not been validated by clinical research, a governing body or academic institution. It has been compiled and published to be a point of reference to educate and assist anyone who is concerned that they, their children, business or community are in the presence of an iPredator or someone in transit to becoming an iPredator.

<u>iPredator Bridge</u>: iPredator Bridge is a theoretical tenet of iPredator representing the psychological, perceptual & behavioral trajectory of people who use Information and Communications Technology (ICT) to harm others. Similar to the iPredator, they are motivated by personal convictions, greed, power, control, <u>narcissism</u> or <u>psychopathology</u>. Different from the iPredator, they have yet to fully engage in criminal/deviant activities using ICT or use complex perceptual distortions to validate the harm they cause.

iPredator Bridge investigates why some people draw near to this nefarious and malevolent realm and either proceed in their maladaptive trajectory or cease and desist. Hidden in cyberspace, and through ICT, they contemplate the benefits and detriments, proceed, and then continue a path where their cognitive and perceptual processes are focused upon directly or indirectly harming others. For those who cross this proverbial bridge, they enter a world where their choices are increasingly governed by criminal, deviant, immoral and maladaptive processes.

Given this writer's strong belief that there are neurochemical, <u>neuropsychological</u>, perceptual and <u>dissociative</u> based changes occurring in all humans who access and interact with ICT and cyberspace, the compilation of all these factors leads to both a new breed of assailant and victim. <u>iPredator Bridge</u> is the connection between the dark aspects of the human mind, ICT, cyberspace and activation of direct or indirect harm towards others. The victim or target of an iPredator may or may not have previously engaged the iPredator Bridge construct himself or herself, and for that matter, may not even know that their loved ones, peers, associates or new online contacts are posturing to become iPredators or actively engaging in iPredator attacks.

Clearly, there is a plethora of <u>contributing factors</u> influencing people to become iPredators. There are also multitudes of factors that influence some people to approach and cross the iPredator Bridge. The harsh reality is that the wonderful abstract universe of cyberspace and the ICT used to enter cyberspace does not come with directions or blueprints on how to prevent being attacked, disparaged or harmed by iPredators.

Based on this writer's research and extensive investigation leading to the creation of the iPredator construct, he and his colleagues have compiled a checklist of warning signs that may suggest a person being queried is approaching the iPredator Bridge, in transit or has fully crossed to the realm of iPredator. The iPredator Bridge Warning Signs Checklist (IBWSC) has not been validated by clinical research, a governing body or academic institution. It has been compiled and published to be a point of reference to educate and assist anyone who is concerned that they, their children, business or community are in the presence of an iPredator or someone in transit to becoming an iPredator.



IBWSC

Note: Responding "Yes, I Agree, True" to any of the statements does not confirm the person being queried is an iPredator or close to becoming one. Responding with an affirmative response should be noted and further investigation is recommended. The term "social networking site" in the IBWSC applies to the multitude of social media sites available online. As of 2012-2013, Facebook, Twitter, Linked In, YouTube, Pinterst and Google + are the most popular social networking sites.

Please be mindful that iPredators use many forums in cyberspace and numerous ICT tools to victimize their targets. In the IBWSC, the term "habitual" represents regular usage of ICT and the Internet. Also in the IBWSC, the acronym, ICT, is defined as Information and Communications Technology and represents an umbrella term consisting of all forms of telecommunication, information technology, broadcast media, audio and video processing, transmission and network based control and monitoring functions.

As stated above, responding "Yes, I Agree, True" to any of the statements does not confirm the person is an iPredator or close to becoming one. However, affirmative responses to five or more of the statements are a strong indicator that the person being queried is an iPredator, either crossing the iPredator Bridge or suffering from some psychological and/or perceptual dysfunction.

- 1. The person is a habitual social networking site and/or ICT user and regularly interacts with a select group of online contacts that he/she has never met in person.
- 2. The person is a habitual social networking site and/or ICT user and has private codes or lingo that is regularly communicated to a select group of followers.
- 3. The person is a habitual social networking site and/or ICT user and has been confirmed posting information that they quickly delete for no apparent reason.
- 4. The person is a habitual social networking site and/or ICT user and has been confirmed posting information that would be considered cryptic or jumbled in content.
- 5. The person is a habitual social networking site and/or ICT user and has been confirmed posting information about other people's offline activities that are innocuous or trivial in nature.
- 6. The person is a habitual social networking site and/or ICT user and has been confirmed to publically post information that excludes someone from being invited to a social activity.
- 7. The person has been confirmed to regularly post information about others in chat rooms, forums or message boards that are trivial and have no social purpose or cause.
- 8. The person has been confirmed to maintain a blog or online public journal that has a central theme with minimal social or creative cause merit.
- 9. The person is a habitual social networking site and/or ICT user and has been confirmed posting images or videos about other people's offline activities and lifestyle.
- 10. The person is a habitual social networking site and/or ICT user and has been confirmed posting messages, images or videos of other people's loved ones not known to the person (i.e. husband wife, children, business, etc.).
- 11. The person is a habitual social networking site and/or ICT user and has been confirmed to maintain his/her identity completely private, yet seems to spend an inordinate amount of time online and/or using their ICT.
- 12. The person maintains a public live journal, blog or website with a central theme not based in any social cause, intellectual or creative endeavor.

- 13. The person is a habitual social networking site and/or ICT user and has been confirmed posting information about other people's offline lives that are considered sensitive or private.
- 14. The person is a habitual social networking site and/or ICT user and has been confirmed to impersonate others and engage with others or post information using their felonious identity.
- 15. The person is a habitual social networking site and/or ICT user and has been suspected of spending more time online or using their ICT than with family, friends, loved ones or peers.
- 16. The person is a habitual social networking site and/or ICT user and has been confirmed encouraging online and offline contacts to invest time or money in unsubstantiated ventures.
- 17. The person is a habitual social networking site and/or ICT user and has been confirmed disseminating information that is felonious about their career, expertise or academic/professional achievements.
- 18. The person is a habitual social networking site and/or ICT user and has been confirmed having multiple usernames with different profile descriptions not explained by internet safety practices.
- 19. The person had been observed turning off, shutting down or closing their ICT when a person unexpectedly approaches them.
- 20. The person has been confirmed to frequent websites, blogs or social networking sites that have been kept secret, discouraged or forbade by loved ones or family members.
- 21. The person spends large amounts of time online and/or using their ICT in private without rational reasons.
- 22. The person spends large amounts of time online, using their ICT, researching what others have posted about them or posting information about others.
- 23. The person has been observed or confirmed exaggerating online about erroneous events and events not crucial to their livelihood.
- 24. The person has been suspected or confirmed to be obsessed with religious, political or philosophical societal movements that they express using ICT.
- 25. The person has been suspected or confirmed to be obsessed with religious, political or philosophical societal movements and spends time in chat rooms, reading and posting information in forums, message boards and comments themed with their cause.
- 26. The person refuses or is hesitant to disclose or discuss their family, career or any offline information leading to their accurate identification.
- 27. The person has been observed or confirmed using ICT to hide their identity or obtain people's identity that has not been legally purchased or downloaded.
- 28. The person has been suspected or confirmed contacting others without a clear reason or obvious connection using ICT.
- 29. The person has been suspected or confirmed contacting others multiple times a day using ICT.
- 30. The person has been observed or confirmed adding "buddies" or "friends" to their social networking site lists, despite not personally knowing them.
- 31. The person has been suspected or confirmed encouraging others to move from public forums to private connections such as email, instant messaging or texting.
- 32. The person has been observed or confirmed asking others, using ICT, for personal information that has little merit for obtaining.
- 33. The person has been observed or confirmed sending online gifts, badges, likes or ± 1 's to others they do not know at social networking sites.
- 34. The person has been observed or confirmed expressing, multiple times, how much they like or despise a person, group or organization using ICT.
- 35. The person has been observed or confirmed changing their personal information to suit the situation or person they are communicating with using ICT.
- 36. The person has been observed or confirmed knowing information about others, but unable or hesitant to disclose how they obtained the information compiled from using ICT.

- 37. The person has been suspected or confirmed connecting with others using ICT, across several different platforms (i.e. Twitter, Skype, Email, etc.), despite not knowing their ICT patterns.
- 38. The person has been suspected or confirmed connecting with people's family, friends or colleagues, despite having no apparent connection to them.
- 39. The person has been observed or confirmed sending or posting disparaging information about others using ICT.
- 40. The person has been confirmed having more than 3 or more online relationships involving an adversarial and/or negative outcome.
- 41. The person has been suspected or confirmed retaliating to negative information being spread about them using ICT.
- 42. The person has been suspected or confirmed sending embarrassing and/or sensitive information to other people's mobile devices or phones.
- 43. The person has been suspected or confirmed engaging in "sexting" with others he/she does not know or much younger or much older than they are.
- 44. The person has been suspected or confirmed engaging in sexual conversations with others they have met online using ICT.
- 45. The person has been suspected or confirmed intermittently spending money at online sex sites.
- 46. The person has been suspected or confirmed regularly responding to contacts from online strangers.
- 47. The person has been suspected or confirmed discussing violent, prejudicial or hate based topics online or using ICT with online contacts or strangers.
- 48. The person has been suspected or confirmed regularly visiting and/or participating in anonymous video or instant messaging chat room sites.
- 49. The person has been suspected or confirmed causing others to log out from chat rooms or instant messaging communicating feeling uncomfortable.
- 50. The person has been observed or confirmed keeping up with news on ICT and/or mobile device security vulnerabilities, despite not having those types of devices.





iPredator was founded in September 2011 to provide educational and advisory products & services to consumers and organizations on <u>Cyber Bullying</u>, Cyber Harassment, <u>Cyber Stalking</u>, <u>Cyber Crime</u>, Internet Defamation, <u>Cyber Terrorism</u>, <u>Online Sexual Predators</u> and the new field they are developing termed, Information and Communications Technology (ICT) Forensic Psychology. Created by a NYS licensed psychologist and certified forensic consultant, <u>Dr. Michael Nuccitelli</u>, their goal is to reduce victimization, theft and disparagement from online assailants.

His partner and iPredator's Chief ICT Investigator, Tina Church, is an Indiana licensed private investigator and founder of the not-for-profit company, The Other Victims Advocacy (TOVA). Together, they have designed a theoretical addition to Dr. Nuccitelli's tech. predator theory of iPredator, called iPredator Bridge. Ms. Church and Dr. Nuccitelli work diligently to help those victimized by iPredators.

In addition to assisting citizens, iPredator's mission is to initiate a national educational & awareness campaign with the help of private, state, and federal agencies. Dr. Nuccitelli can be reached at Dr@TechPredator.com. iPredator's criminal psychology & forensics blog can be viewed at www.DarkPsychology.co and their website, www.iPredator.co, offers site visitors an enormous database on Cyber Criminal Psychology, Internet Safety and iPredators. Although iPredator has joined a multitude of social networking sites, feel free to visit their social sites planned to be their major information and announcement vehicles.

Facebook: <u>The iPredator</u>
Google +: <u>The iPredator</u>
Linked In: <u>iPredator</u>
Twitter: <u>TheiPredator</u>
YouTube: <u>iPredator</u> Team

For online users seeking Internet and cyber-attack protection, please read about iPredator's innovative advisory-based membership service called, <u>iPredator Protected</u>. With the growth and expansion of social media, Dr. Nuccitelli and iPredator offers a unique assessment service called the <u>iPredator Facebook Safety Analysis</u>. In addition to offering advice, education and investigation, Dr. Nuccitelli has designed 13 checklists (<u>IISC Collection</u>) that can be taken online and 26 checklists and inventories (<u>IISC & IPI Collection</u>) that can be purchased. All of Dr. Nuccitelli's checklists and inventories were designed for assessment, education and prevention education (<u>IISC & IPI Collection Overview.</u>) To reach iPredator and Dr. Nuccitelli, please contact them by email at <u>Dr@TechPredator.com</u> or calling (<u>347</u>) 871-2416.