CSII

Cyber Stalker Identification Interview

Michael Nuccitelli, Psy.D.

www.ipredator.co

CSII

Cyber Stalker Identification Interview

The Cyberstalker Identification Interview (CSII) is an internet safety tool and cyberstalker identification assessment authored by Michael Nuccitelli, Psy.D., a New York State licensed psychologist and iPredator construct creator. The CSII helps an online user to assess his/her online risk activities, cyber-attack vulnerabilities and the identity of a cyberstalker if being targeted.

Designed to be multi-functional, the CSII is a structured identification interview for education, investigation and data collection. The CSII can also be used for compiling evidentiary information for law enforcement, Internet Service Providers and the legal system if the online user is looking to identify a cyberstalker.

CSII

Cyber Stalker Identification Interview

NOTE: The CSII has been designed to investigate the vulnerabilities of an online user being cyberstalked or harassed, to locate and/or identify the identity of an unknown cyberstalker and compile data of a known or suspected cyberstalker in which data collection is vital for reporting to authorities and compiling evidence for legal representatives. Based on the rational for completing the CSII, the person conducting or completing the interview is recommended to interpret the questions as follows:

I. If the cyberstalker is known or his/her identity is suspected, the questions are straight forward and formatted for this event.

II. If the identity of the cyberstalker is unknown, the questions should be premised with, "If the cyber stalker were known," and then read the question and note responses accordingly.

III. Whether the cyberstalker is known or unknown to the target, careful analysis of the target's responses will yield their ICT vulnerabilities and high-risk ICT behaviors.

CSII TERMS

I. CS: A suspected, alleged, confirmed or unknown person or group engaged in cyberstalking another person, group or organization using information and communications technology.

II. Target: A person, group or organization that is being taunted, harassed, disparaged or abused using information and communications technology (ICT) by a suspected, alleged, confirmed or unknown person or group.

CSII QUESTIONS

1. Does the CS have a motive or suspected motive? (Note examples whether factual or alleged.)

2. Are the harassing threats or central themes sexual, obsessive or violent in nature or a combination of the three? (Note examples whether factual or alleged.)

3. Has the CS posted and/or disclosed personal information about the target that the target is unable to understand how the CS obtained the personal information? (Note examples.)

4. Has the CS ever followed or suspected of following the target appearing in their home or place of business? (Note when, where, how often and last reported incident.)

5. Has the CS persuaded other ICT users into harassing or threatening the target by using online bulletin boards or chat rooms? (Note examples and/or names of websites.)

6. Has the CS posted a controversial or enticing message online under the name, phone number or e-mail address of the target? (Note examples and/or names of websites.)

7. Does the target live in a region that has a Stalking/Cyber Stalking Unit working for or affiliated with their law enforcement authorities? (Note contacts and actions taken.)

8. Does the target save all CS communications for evidence and actively compile a record of the cyberstalking events with Internet Service Providers (ISP) to give authorities? (Note contacts and ISP actions taken.)

9. Has the CS stalked the target via chat rooms, message boards and discussion forums or via e-mail messages? (Note examples and/or names of websites or content in emails.)

10. Is the CS trying to connect, intimidate, humiliate or control the target? (Note examples whether factual or alleged.)

11. Has the CS made harassing phone calls, left written messages or vandalizing the target's property? (Note examples and target's response.)

12. Has the target experienced any of the following: threatening or obscene e-mail, spamming, text messaging harassment, finding improper messages on message boards or in guest books, receiving electronic viruses or electronic identity theft? (Note examples and target's response.)

13. If the target knows or suspects one or more people to be the CS, has the target sent both a hard copy and electronic warning to those suspected of being the CS? (Note examples, target's initiatives and CS response.)

14. Has the target filed a report with local law enforcement or contacted their local prosecutor's office to see what charges can be pursued, when they can identify the CS? (Note examples and the authorities' response.)

15. Has the CS terrorized the target by impersonating them in chat rooms and online bulletin boards by posting their telephone number, address or other personal information? (Note examples and/or names of websites and content of information disclosed.)

16. Has the CS's identity been concealed by using different Internet Service Providers (ISP) and/or by adopting different screen names? (Note examples and tactics used.)

17. Has the CS used anonymous re-mailers that make it all-but-impossible to determine the source of an e-mail or other electronic communication? (Note examples and tactics used.)

18. Has the target experienced electronic monitoring such as spyware, bugging or video surveillance? (Note examples and tactics used.)

19. Has the target been sent manipulative, threatening, lewd or harassing emails from an assortment of email accounts? (Note examples and tactics used.)

20. Has the CS hacked into any of the target's online accounts (such as banking or email) and changed their settings and passwords? (Note examples and password complexity hacked.)

21. Has the CS created false online accounts on social networking and dating sites, impersonating the target or tried to set up contact with the target by using a false persona? (Note examples and names of false personas.)

22. Has the CS signed the target up to many online mailing lists and services using the target's name and email address? (Note examples and/or names of lists and services.)

23. Has a background check been performed on the suspected CS or pool of potential CS's? (If yes, give conclusions and if not, why not.)

24. Has the cyberstalking extended to portable devices such PDAs (Personal Data Assistants) or mobile devices? (Note examples and tactics used.)

25. Is the CS believed to be or have been confirmed to be driven by revenge, hate, anger, jealousy, obsession or mental illness? (Note examples.)

26. Is the CS believed to be driven by the desire to frighten or embarrass the target? (Note examples whether factual or alleged.)

27. Has the CS posted comments on social networking sites intended to cause the target distress or humiliation? (Note examples.)

28. Has the CS sent a stream of unsolicited messages (hateful or provocative) to the target or to associates of the target? (Note examples.)

29. Has the CS sent or posted offensive comments or lies using their own identity or impersonating the target? (Note examples.)

30. Has the CS hacked or taking over the target's computer or email accounts? (Note examples.)

31. Has the CS changed the target's password and blocked their account? (Note examples.)

32. Has the CS signed the target up for spam, pornography sites or questionable sales offers? (Note examples.)

33. Has the CS followed the target into cyber chat rooms or discussion boards? (Note examples.)

34. Has the CS created sexually explicit images of the target and/or posted them on web sites or commercial pornography sites? (Note examples and/or names of websites.)

35. Has the CS ever tried to lure or entice the target into an offline meeting? (Note examples.)

36. Has the target installed or considered installing a monitoring system that can capture data from all their information and communications technology? (Note examples.)

37. Has the CS used direct, indirect or a combination of cyberstalking methods? (Note examples.)

38. What are the target's state cyberstalking and cyber harassment laws? (Note statutes and reasons if not known.)

39. If the CS has been identified or known, what is the CS's state cyberstalking and cyber harassment laws? (Note statutes and reasons if not known.)

40. Is it possible the CS is cyberstalking the target for profit or for competitive advantage? (Note examples whether factual or alleged.)

41. What evidence would suggest the CS is or is not cyberstalking the target for profit or for competitive advantage? (Note examples.)

42. Has the CS cyberstalked and/or harassed the target's coworkers? (Note examples.)

43. Has the CS cyberstalked and/or harassed the target's family? (Note examples.)

44. Has the CS cyberstalked and/or harassed the target's customers? (Note examples.)

45. If applicable, has the CS cyberstalked and/or harassed the target's fans, listeners and/or viewers? (Note examples.)

46. Is the relationship between target and CS better classified as affectionate & amorous or persecutory and angry? (Note examples.)

47. Is the nature of the relationship between CS and target personal, professional, employment, media, acquaintance, known or unknown? (Note examples whether factual or alleged.)

48. If the nature of the relationship between CS and target is unknown, would a best guess estimate be personal, professional, employment, media or acquaintance and why? (Note examples whether factual or alleged.)

49. If a CS has been suspected or believed to be a CS, is there any evidence via historical data and/or a background check if they ever suffered from any type of psychiatric and/or substance abuse disorder or criminal history? (Note examples whether factual or alleged.)

50. If a CS has been identified or suspected of being the CS, is the nature of the relationship between the CS and target domestic or non-domestic? (Note examples.)

51. If a CS has been identified or suspected of being the CS, is the nature of the content of the communications non-delusional or delusional? (Note examples.)

52. If a CS has been identified or suspected of being the CS, is the level of risk to the target in terms of aggression evaluated to be low, medium or high? (Note examples whether factual or alleged.)

53. If a CS has been identified or suspected of being the CS, is the motive of the CS most likely to be motivated by infatuation, possession or anger/retaliation? (Note examples whether factual or alleged.)

54. If a CS has been identified or suspected of being the CS, have they had an intimate relationship with the target? (Note examples and last intimate event and outcome.)

55. If a CS has been identified or suspected of being the CS, is the CS a family member or close friend? (Note examples and if relative is a blood relative.)

56. If a CS has been identified or suspected of being the CS, is the CS a family member, close friend or ex-intimate partner who views the relationship as unacceptable? (Note examples.)

57. If a CS has been identified or suspected of being the CS, is the CS a family member, close friend or ex-intimate partner's behavior characterized by a mixture of revenge and desire for reconciliation? (Note examples.)

58. If a CS has been identified, have they tried to bring to fruition an intimate relationship with the target? (Note examples.)

59. If a CS has been identified or suspected of being the CS, have they mistakenly perceived the target will reciprocate their love and/or affections? (Note examples.)

60. If a CS has been identified or suspected of being the CS, do they fail to abide by social rules governing courtship? (Note examples.)

61. If a CS has been identified or suspected of being the CS, are they intellectually limited and/or socially incompetent? (Note examples.)

62. If a CS has been identified or suspected of being the CS, do they harass the target with the specific intention of causing them fear and apprehension out of a desire for retribution for some actual or supposed injury or humiliation? (Note examples.)

63. If a CS has been identified or suspected of being the CS, do they cyber stalk for information gathering purposes or fantasy rehearsal in preparation for a sexual, deviant or criminal attack? (Note examples.)

64. If a CS has been identified or suspected of being the CS, is there any evidence that they are not a composed cyber stalker or Internet troll experiencing pleasure from harassing and stalking the target? (Note examples.)

65. If a CS has been identified or suspected of being the CS, is there any evidence the harassment started over a trivial debate or discussion, which blew up out of proportion? (Note examples.)

66. If a CS has not been identified, is there any recollection by the target of recent trivial debate or discussion that blew up out proportion? (Note examples.)

67. Does the target report receiving bizarre comments, rambling conversations, unclear unrelated comments, intimidating multimedia images and/or sounds from the CS? (Note examples.)

68. Does the target report the CS is not seeking to establish a relationship, but wishes to cause them distress? (Note examples.)

69. Does the target report the CS issue threats, apologies or reconciliation? (Note examples.)

70. If a CS has not been identified or the CS is unknown, is there any evidence the CS's harassment is an attempt to 'win' the feelings and/or gain the attention of the target? (Note examples.)

71. Does the CS demonstrate detailed knowledge about the target? (Note examples.)

72. If the target suspects more than one CS, has the group of CS's perceived that they had been 'wronged' and wishes to 'punish' the target? (Note examples.)

73. If the target suspects more than one CS, has the group of CS's used similar stalking methods or similar stalking themes? (Note examples.)

74. If the target suspects more than one CS and the target has an idea who the CS's may be, do they share some similar attributes the target or the target's employer or affiliated organization have opposed? (Note examples.)

75. If the target suspects more than one CS, does this group of CS's share any similar attributes to the target or the target's employer or affiliated organization? (Note examples.)

Michael Nuccitelli, Psy.D.

Michael Nuccitelli, Psy.D. is a NYS licensed psychologist, cyberpsychology researcher and online safety educator. In 2009, Dr. Nuccitelli finalized his dark side of cyberspace concept called iPredator. Since 2010, he has advised those seeking information about cyberbullying, cyberstalking, cybercriminal minds, internet addiction and his Dark Psychology concept. By day Dr. Nuccitelli is a practicing psychologist, clinical supervisor and owner of MN Psychological Services, PLLC. After work and on the weekends, he volunteers helping online users who have been cyber-attacked. Dr. Nuccitelli's is always available to interested partied and the media at no cost. The iPredator website and everything created by Dr. Nuccitelli is educational, free and public domain.