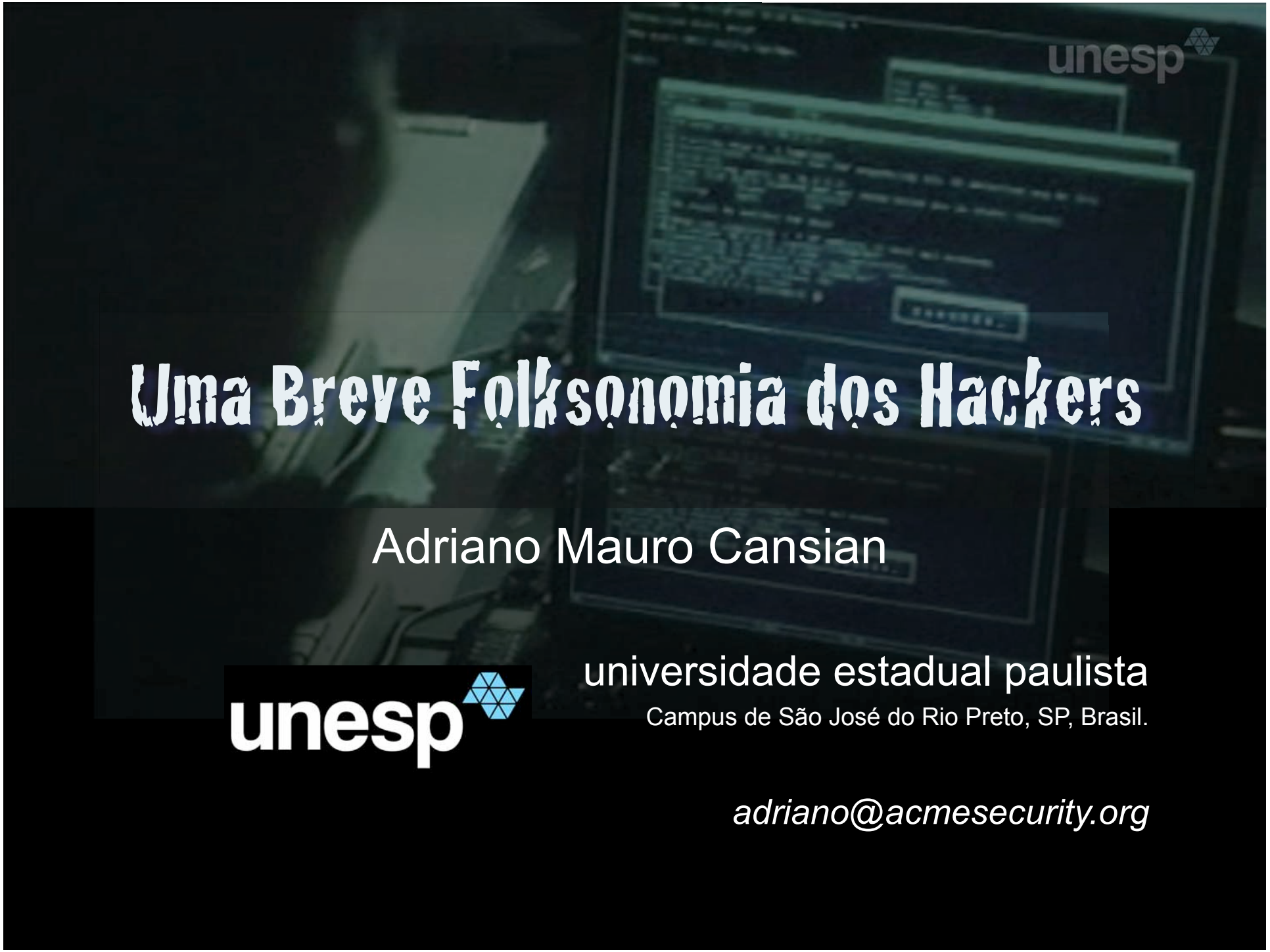


Uma Breve Folksonomia dos Hackers

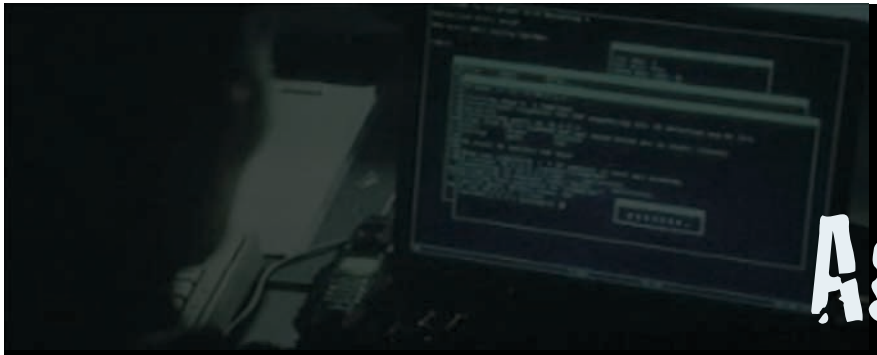
Adriano Mauro Cansian

unesp

universidade estadual paulista

Campus de São José do Rio Preto, SP, Brasil.

adriano@acmesecurity.org



Agenda

- Introdução.
  - Motivação, problemas e desafios.
- Evolução do termo "*hacker*".
- A Folksonomia.
- Psicologia e criminologia.
- Conclusões

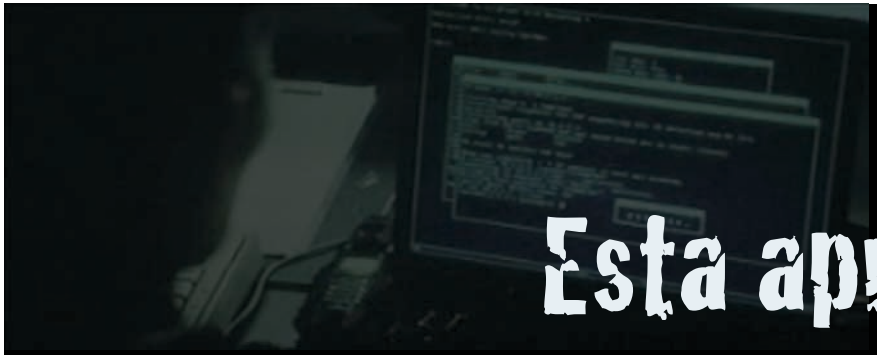
Folksonomia (folksonomy)

: junção de duas palavras "*folk*" (povo, gente) e "taxonomia".

"classificação do povo"

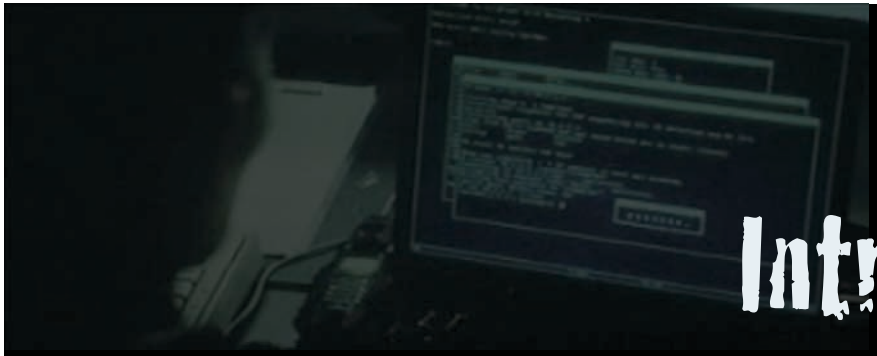
não deve ser associada com a classificação de pessoas em si, e sim com classificação feita por pessoas.

- Thomas Vander Wal, atual membro do *Web Standards Project*.



Esta apresentação...

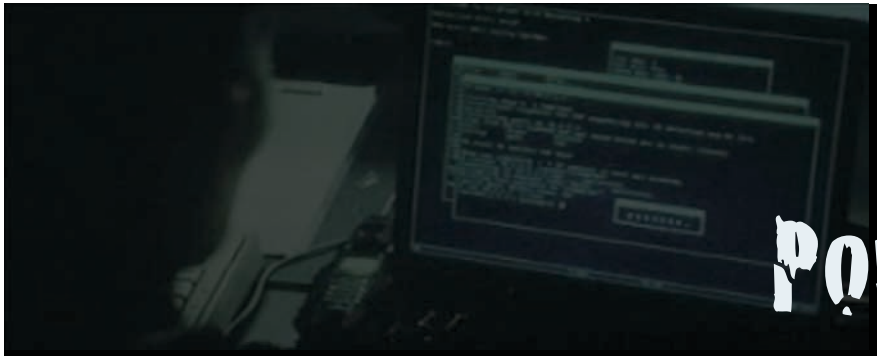
- ... é:
  - Experimental;
  - Investigativa;
  - Uma Pesquisa.
- ... não é:
  - Julgamento;
  - Endosso;
  - Verdade absoluta.



unesp

Introdução

- *Criminal Hackers*: inimigo #1 *IT Security.*
- Relatórios dão conta de grandes perdas.
- O que sabemos sobre “eles” ?
  - Perfilização pouco eficiente.
  - Generalização exacerbada.
  - Mistificação.
  - Folclore.
  - Poucas ações práticas.

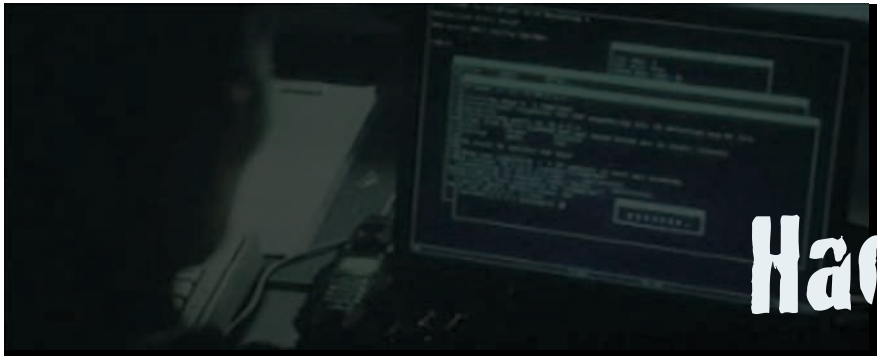


Por quê ?

- Entendimento do comportamento.
- Evitar estereótipos.
- Aprender sobre o atacante
  - Identificar as ameaças.
  - Elaborar a defesa.
  - Separar *good guys* X *bad guys*.

Alguns estudos

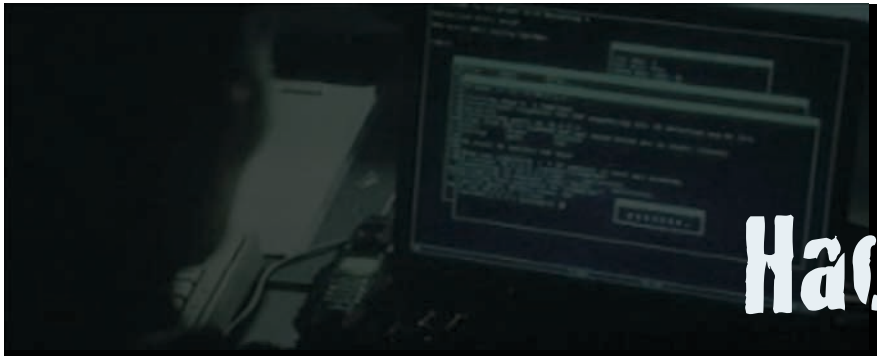
- Landreth (1985)
- Hollinger (1988)
- Sterling (1992)
- Chantler (1996)
- Rogers (1997)
- Power (1998)
- Parker (1998)
- Adamski (1999)
- Voiskounsky (2003/2007)



Hacker (i)

- *Hacker* : Tornou-se termo genérico.
- Refere-se a uma comunidade diversa:
  - Crackers, gurus, coders, script kiddies, programmers, criminosos, cyberpunks, ativistas, etc.. etc...

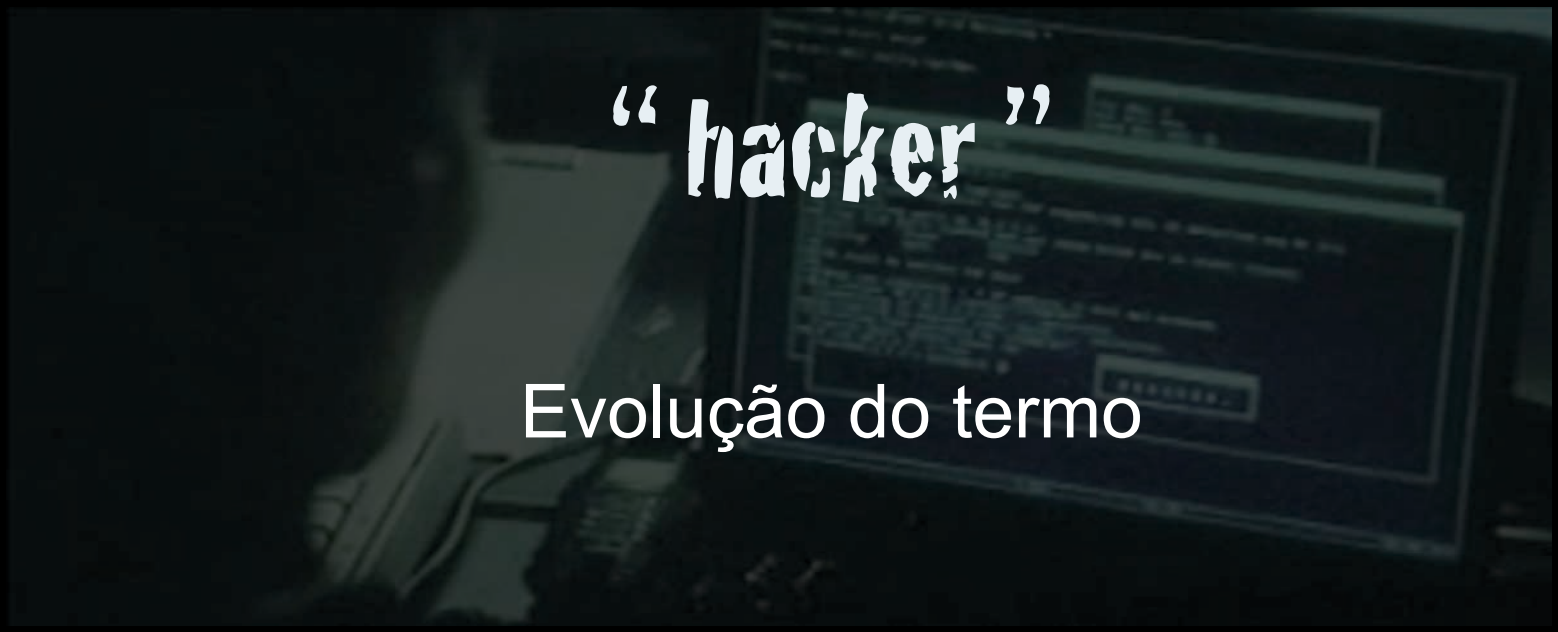
" Para se tornar um hacker, simplesmente autodenomine-se um. "



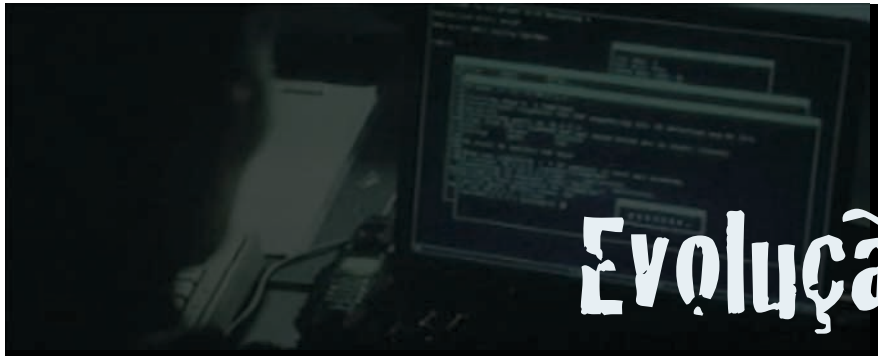
Hacker (2)

Descreve a **atividade envolvida**, mas não reflete as diferenças entre indivíduos engajados.

- Grupo altamente heterogêneo.

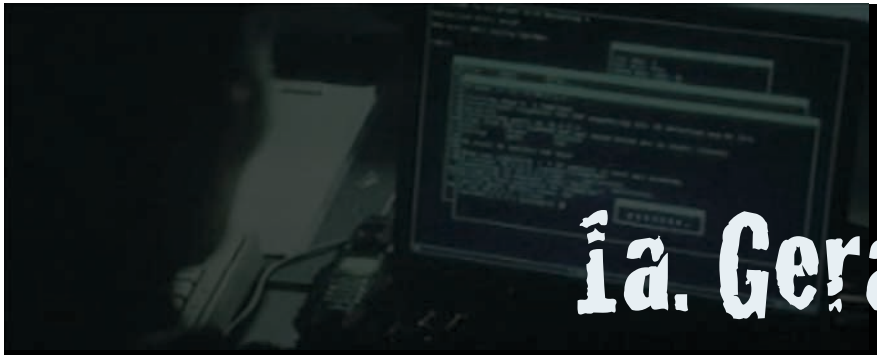


Evolução do termo



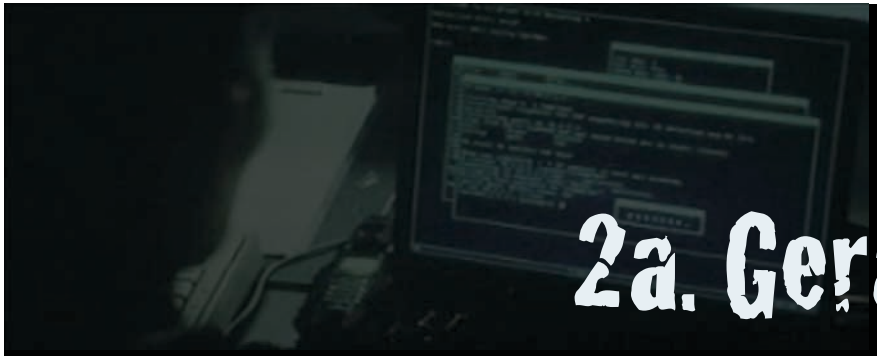
Evolução do termo

- Cinco gerações “hacker”
  - 1G : Grandes Programadores MIT/Stanford (60’s).
  - 2G : (R)Evolucionários (70’s).
  - 3G : Players (80’s).
  - 4G : Criminosos & Cyberpunks (90’s).
  - 5G : Cyberterror (00’s).



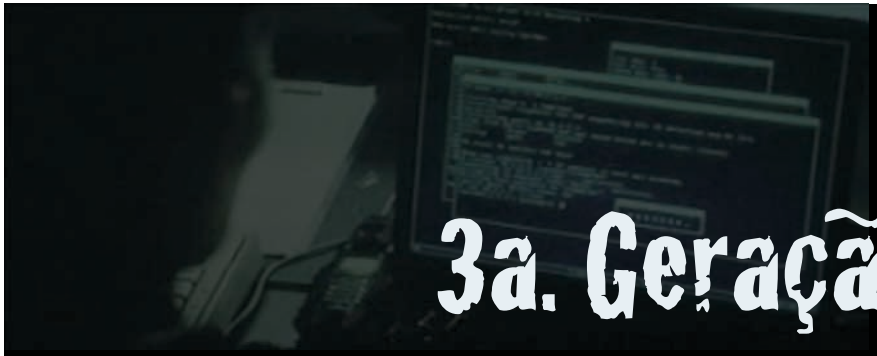
1a. Geração – 60's

- Grandes programadores e cientistas.
- Métodos inovativos de programação.
- Ética hacker (*Do The Right Thing*)
- Muito respeitados (Gurus)
- MIT (TMRC) & Stanford (SAIL)
  - *Tech Model Railroad Club* (TMRC): 1946
  - *Stanford Artificial Intelligence Laboratory*: 1963
    - http://en.wikipedia.org/wiki/TMRC
    - http://en.wikipedia.org/wiki/Stanford_Artificial_Intelligence_Laboratory



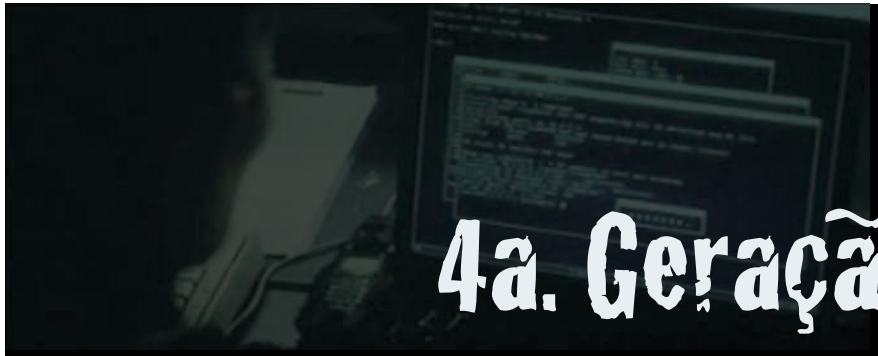
2a. Geração – 70's

- (R)evolucionários da computação.
- *Hardware Hackers.*
- **Transição de Mainframes para computação pessoal.**
  - *Computer Kits* (Altair, Apple).
- Fundação das grandes Cias.
  - Muita Pirataria de software.
  - Atividade criminal menor: *Phreaking, Blue Boxing.*



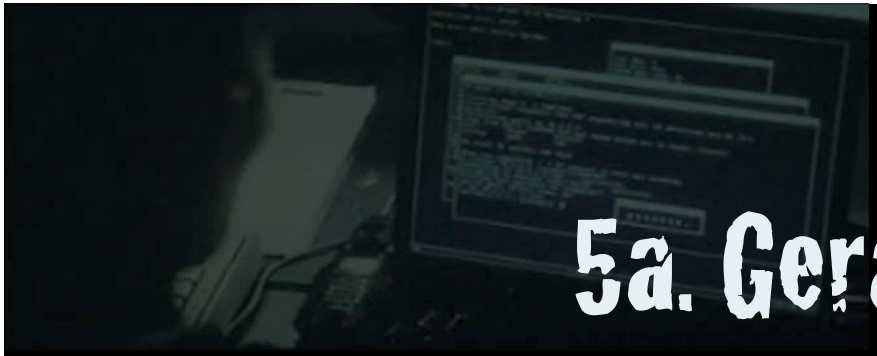
3a. Geração – 80's / 90's

- *Players*
  - Computadores pessoais (PC).
  - Explosão das redes.
  - Entretenimento.
    - *Hacking for fun.*
    - *Hacker's Wars.*
  - Privacidade, vingança, curiosidade...
  - Atividade criminal menor.



4a. Geração – 90's / 00's

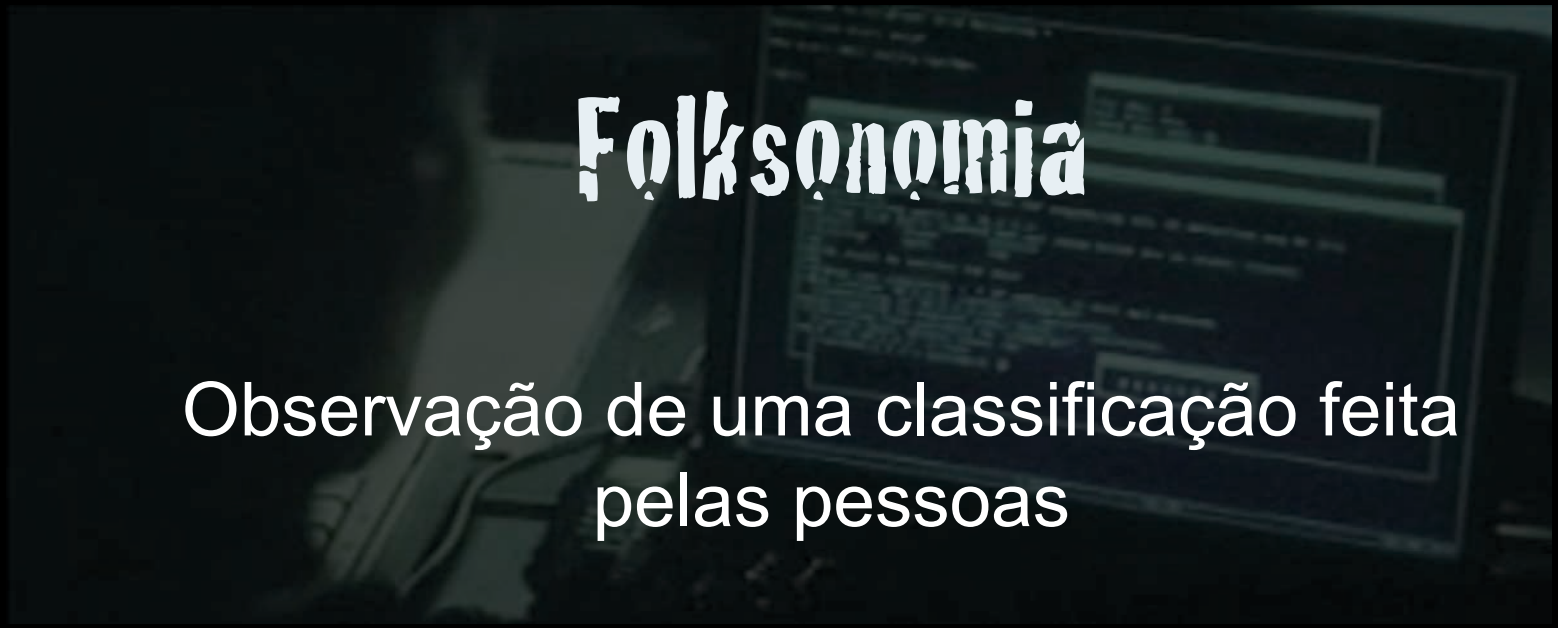
- Criminosos.
  - Motivação financeira, crime organizado.
- Raramente participam da elite técnica.
  - Motivados primariamente por: poder, projeção, vingança, ódio, intenção maliciosa.
- Não respeitados.
- Grande atividade criminosa.



5a. Geração – 00's

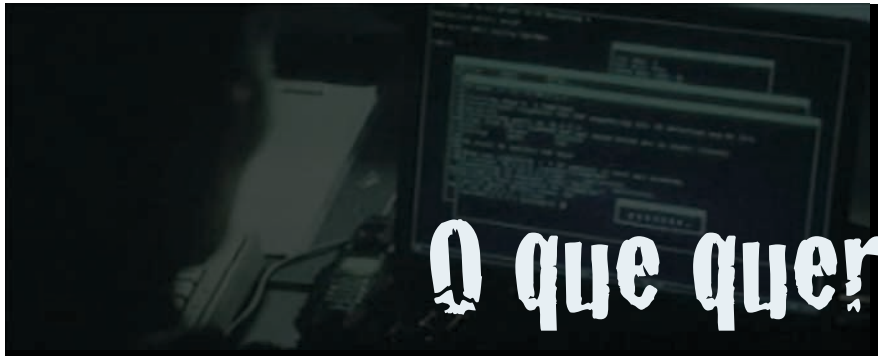
- Cyberterror.
  - Geopolítica.
  - Disputas ideológicas
  - Disputas entre nações.
- Vantagens competitivas:
  - Econômicas, políticas, estratégicas.

unesp



Folksonomia

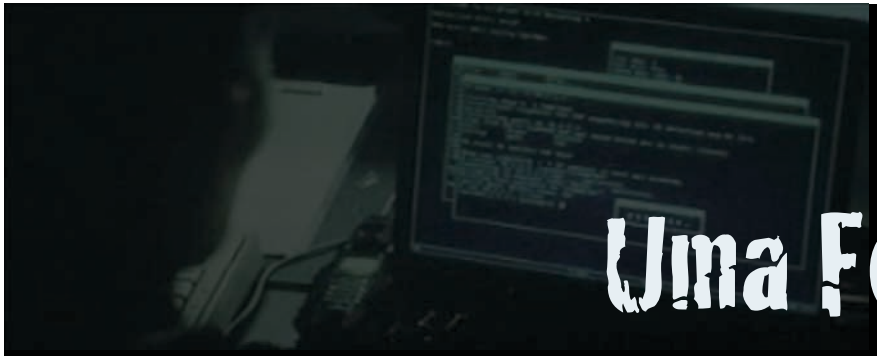
Observação de uma classificação feita pelas pessoas



O que queremos delimitar

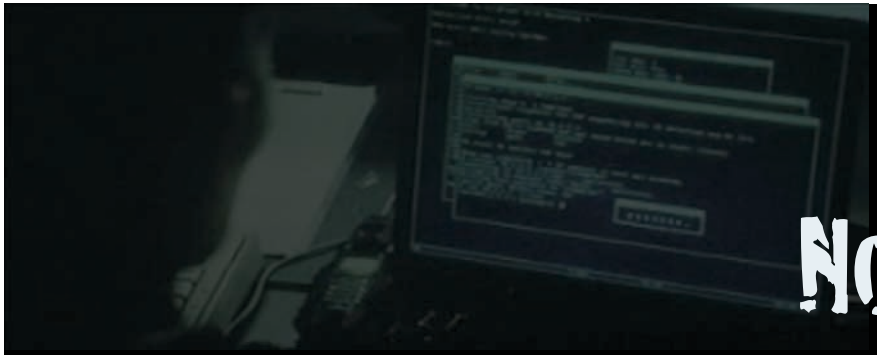
- *Hackers*, *phreakers*, *crackers*, etc..., etc...
- Evitar generalização "*hacker*".
  - Foco em pesquisa sobre criminologia geral.

- Observar amplo espectro de atividades.
  - Quais grupos estão envolvidos.
  - Outras definições operacionais.
  - Qual o perfil.



Uma Folksonomia

1. Novatos (*Script Kiddies*).
2. *Crackers* ou *Cyberpunks*.
3. *Coders*.
4. *Insiders*.
5. Velha Guarda.
6. Profissionais.
7. Cyber-terroristas.

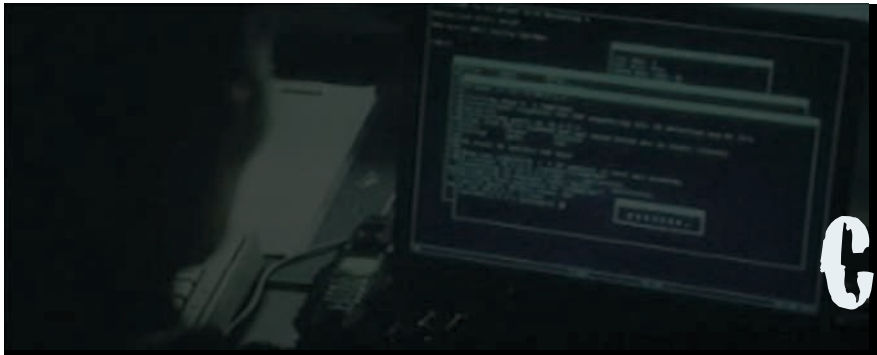


Novatos

- *Script Kiddies / Newbies / Wannabe's.*
  - Habilidades computacionais limitadas.
  - "*Google is my master*".
- Podem causar danos extremos.
  - Pois não entendem como o ataque funciona.
- Grande atenção da mídia.

Crackers ou Cyberpunks

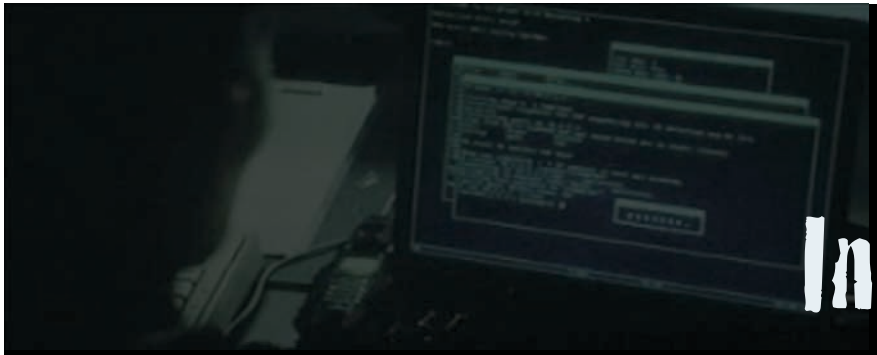
- Melhores habilidades computacionais.
- Conhecimento de programação: limitado.
- Melhor entendimento sobre como os ataques funcionam.
- Misturam: intenção criminal, comportamento malicioso, fraudes, ódio, revanche, diversão.
- Grande atenção da mídia.



unesp

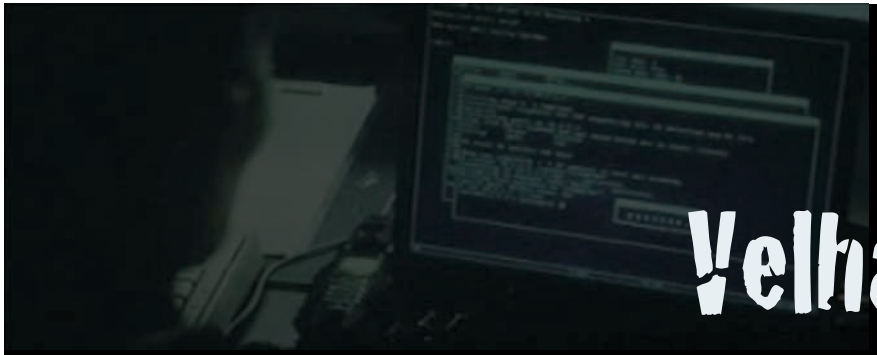
Coders

- Tecnicamente muito habilidosos.
- Escrevem ferramentas.
  - Distribuem livremente.
- Atuam como mentores.
- Motivados por senso de poder e prestígio.
  - Reverenciados.
- Em alguns casos: perigosos.
  - Agendas secretas, interesses, militância.



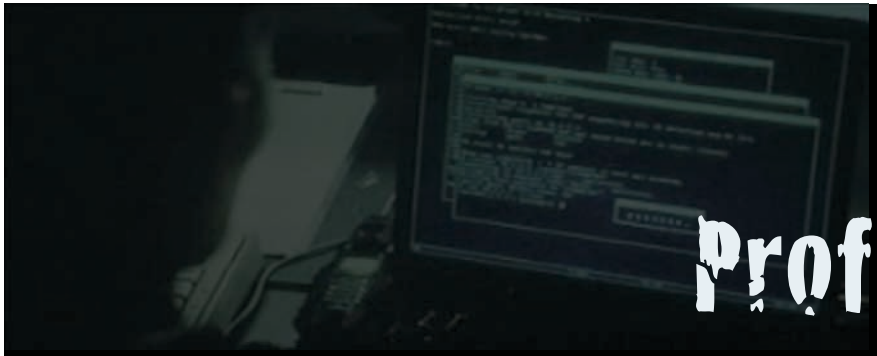
Insiders

- Letrado em computação e habilidosos.
- Atuação em TI.
- Funcionário descontente / ex-funcionário.
- Privilégios da posição facilitam o ataque.
- Maior problema atual de segurança:
  - Envolvidos em 70 a 80% dos casos de fraudes.



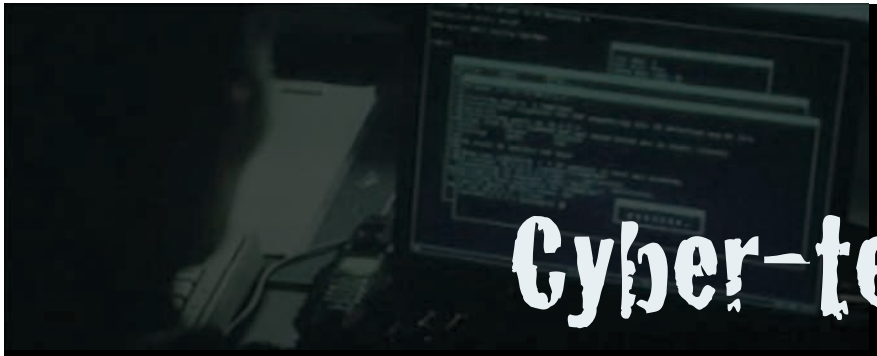
Velha Guarda

- *Old Hackers*.
- Sem nenhuma intenção criminal ou danosa.
- Valores iguais à 1ª. Geração de hackers.
  - Alguma ausência de respeito à propriedade privada ☺
- Mentores.
- Bastante defensivos.



Profissionais

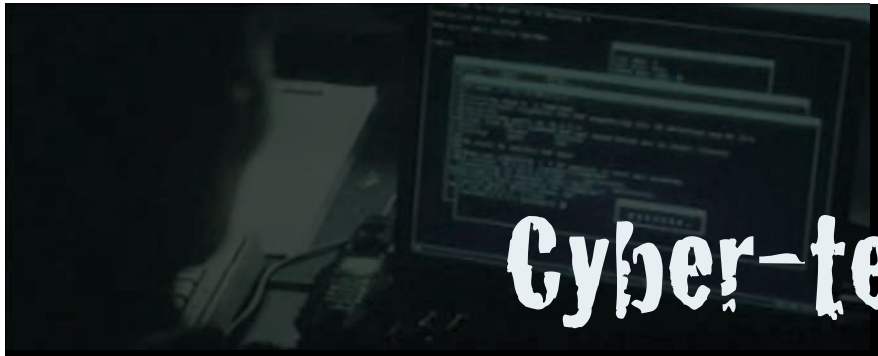
- Criminosos Profissionais.
  - Envolvidos com Crime organizado.
  - Espionagem corporativa.
  - "*Hitmen*".
- Altamente motivados.
  - Algumas vezes bem treinados.
- Bem financiados.
  - Com acesso a recursos sofisticados.
- Há pouco conhecimento sobre este grupo.



Cyber-terroristas (i)

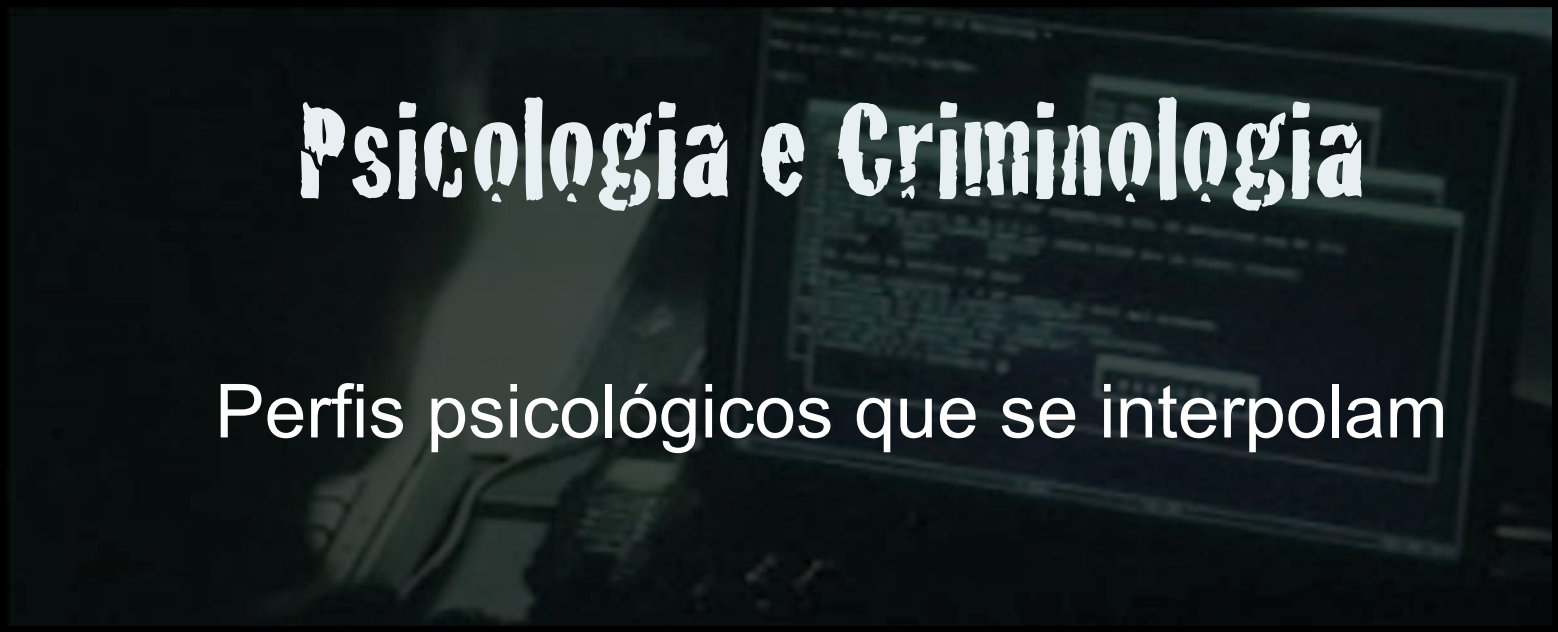
- Ascensão da espionagem e ataques virtuais.
  - A nova guerra fria virtual: China na vanguarda.
- Infra-estruturas nacionais sob ataque.
  - Ataques virtuais mais sofisticados.
  - Organizadas para espionagem política, militar, econômica e técnica.

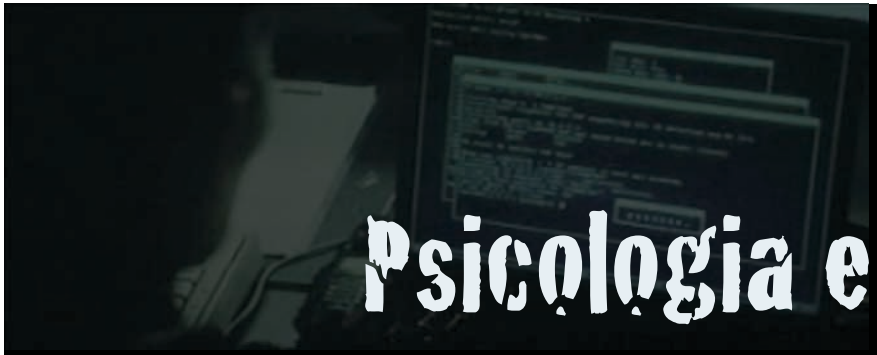
McAfee Relatório de Criminologia Virtual.
http://www.mcafee.com/us/research/criminology_report/default.html



Cyber-terroristas (2)

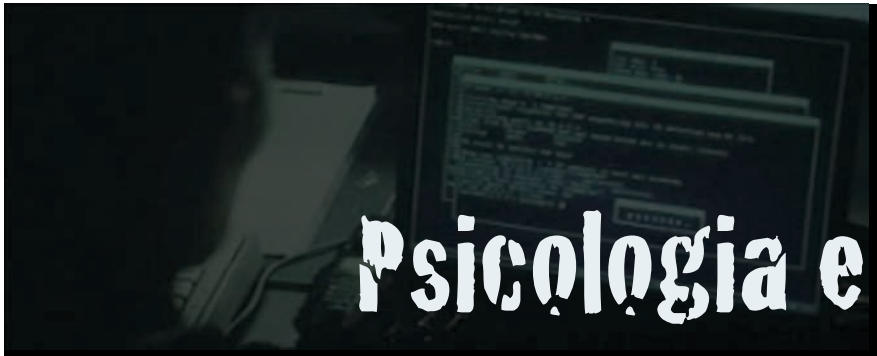
- Crescimento de atividade desde a queda de várias agências do leste europeu no final dos 90's.
  - Motivados e bem financiados.
- Misturam retórica política com atividade criminosa.
- Ataques bem orquestrados.
- Há pouco conhecimento sobre este grupo.


Psicologia e Criminologia
Perfis psicológicos que se interpolam



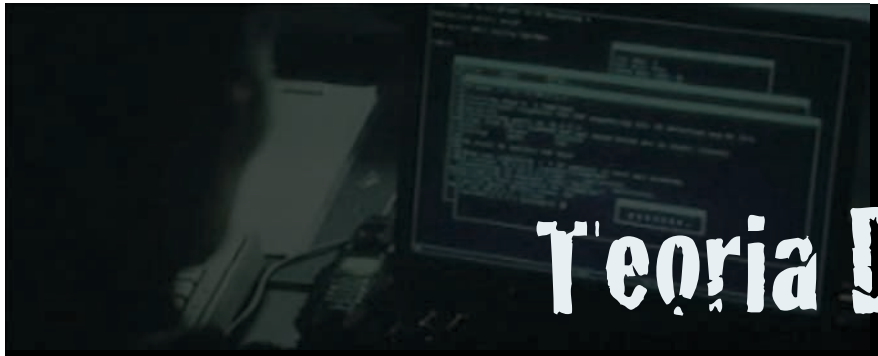
Psicologia e Criminologia (i)

- Estudos psicológicos e criminológicos dificultados por diversos fatores.
- Não possuem evidências corroborativas.
  - Subconjunto limitado da comunidade.
    - Pouca representatividade.
    - Espaço amostral pequeno.
  - Dificuldades etnográficas.
  - Meio inadequado.
- Não podem ser generalizados.



Psicologia e Criminologia (2)

- Teorias mais aceitas:
  - Teoria Desviante.
    - Associação Diferencial.
    - Desimpedimento moral.
    - Teoria de aprendizagem social.

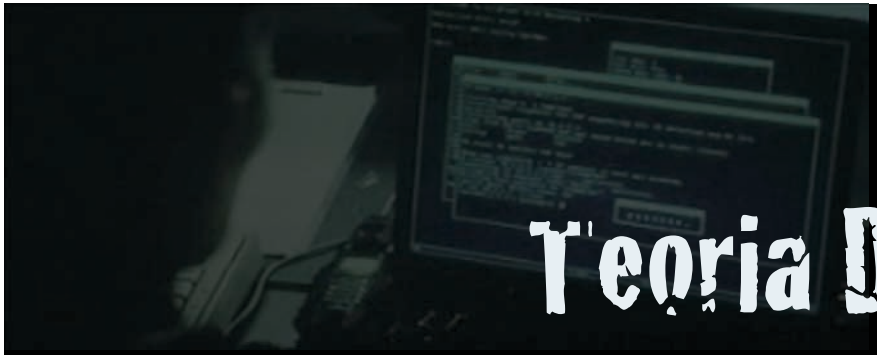


Teoria Desviante (i)

Teoria desviante:

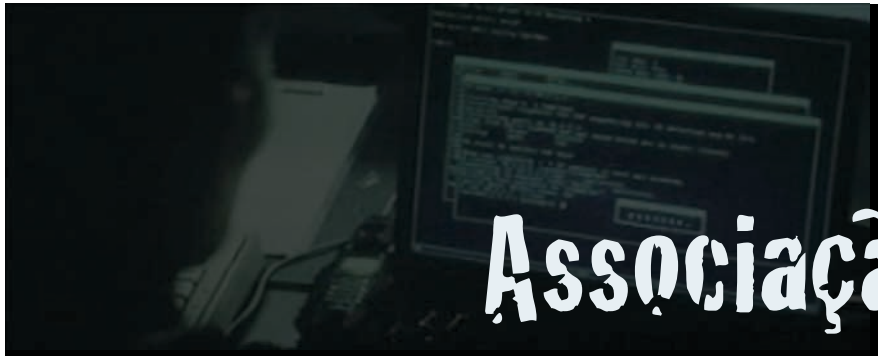
estuda ações ou comportamentos que violam normas culturais, incluindo leis formais (e.g. crimes), bem como violações informais de normas sociais.

http://en.wikipedia.org/wiki/Deviant_behavior



Teoria Desviante (2)

- Perfis de Psicologia e criminologia.
  - Como os indivíduos se envolvem em comportamento delinqüente?
  - Como justificam o comportamento?



Associação Diferencial

- Defende que o comportamento criminal **não** é inerente a um indivíduo em particular.
  - **É aprendido.**
- Delinqüência baseada em conflito normativo.
  - Definições conflitantes do comportamento apropriado.
- Conflito de normas e definições.

Desimpedimento Moral (i)

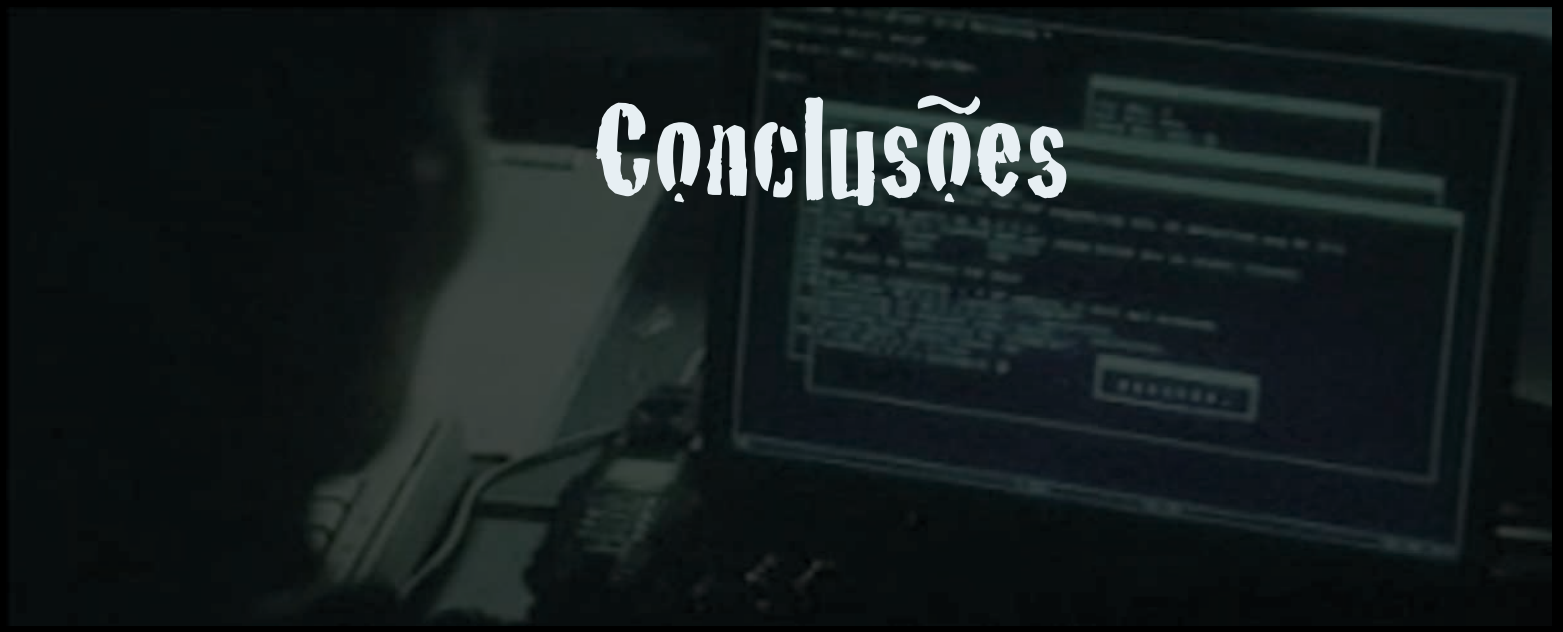
(*Moral Disengagement*)

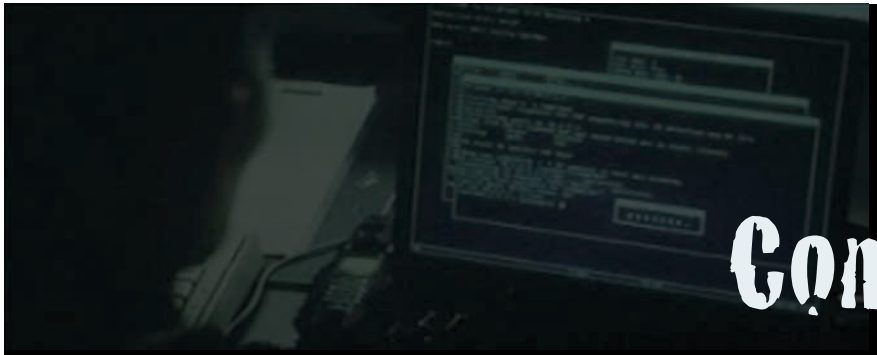
- Processo de **auto-convencimento** de que padrões éticos não se aplicam a si próprio, num contexto particular.
- Psicologicamente separa as reações, desabilitando os mecanismos de auto-condenação.

Desimpedimento Moral (2)

(Moral Disengagement)

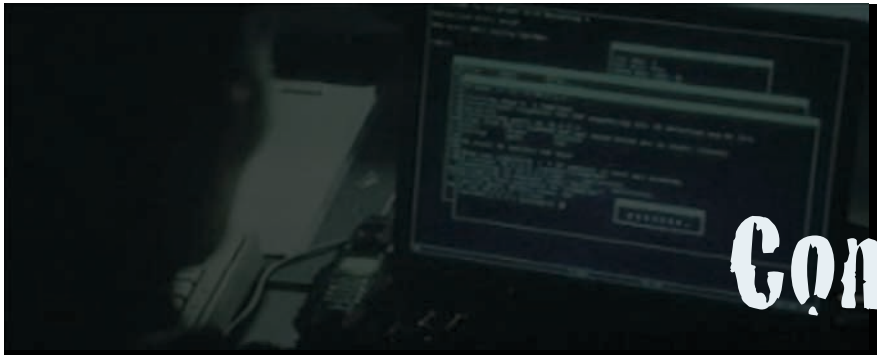
- Mecanismos:
  - Justificativa moral.
  - Minimização, ignorância ou desconstrução das conseqüências.
  - Desumanização.
  - Atribuição de culpa sobre as vítimas.
- Valorização de suas próprias ações sociais ou propósitos morais.
  - Robin Wood.


Conclusões



Conclusões

- Pesquisa empírica.
- Objetividade de vários estudos é questionável.
- Descobertas sobre um grupo não generalizável para outro grupo.
  - Apesar de que grupos se interpolam.



Conclusões

- Criminoso ≠ *hacker* ≠ cyber-terrorista.
- Existe uma nova geração de criminosos.
  - Sub-grupo específico.
- **Pouco conhecimento sobre os grupos realmente problemáticos.**
- **Teorias e perfis psicológicos parciais.**

Não existe *profile* genérico
para um hacker.

Adriano Mauro Cansian

Laboratório ACME! de Pesquisa em Segurança de Redes
UNESP - Universidade Estadual Paulista

http://www.acmesecurity.org

adriano@acmesecurity.org

PGP KeyID: **0x3893CD2B**