

WIDDERSHINS: THE HACKER NATION



SIMPLE NOMAD
DEFCON X - 2002

H A T E

ABOUT ME/THIS TALK



NMRC
BindView
Skills Needed

L O V E

THE YEAR IN REVIEW



DMCA muscle is flexed.

Terrorism.

Legislation clarifies various portions of previous laws.

More knee-jerk legislation on the way.



THE PROBLEM: PACKETEERING SATAN'S NETWORK



extreme conditions demand extreme solutions

(Programming Satan's Computer - Ross Anderson and Roger Needham 1995)

WHAT CAN SATAN SNIFF?

"Anonymous Re-mailers as Risk-Free International Infoterrorists" presented by Paul Strassmann, National Defense University and William Marlow, Science Applications International Corporation. Presented at the "Information, National Policies, and International Infrastructure" conference at Harvard Law School, Cambridge, Massachusetts, January 30, 1996.



<http://www.strassmann.com/pubs/anon-remail.html>

<http://ksgwww.harvard.edu/iip/GIIconf/gii2age.html>

<http://catless.ncl.ac.uk/Risks/17.87.html#subj6>

During the question and answer session, an interesting discussion ensued. Here is a quote from conference attendee Viktor Mayer-Schoenberger:

"Both presenters explicitly acknowledged that a number of anonymous remailers in the US are run by government agencies scanning traffic. Marlow said that the government runs at least a dozen remailers and that the most popular remailers in France and Germany are run by the respective government agencies in these countries. In addition they mentioned that the NSA has successfully developed systems to break encrypted messages below 1000 bit of key length and strongly suggested to use at least 1024 bit keys. They said that they themselves use 1024 bit keys."

WHAT CAN SATAN SNIFF?



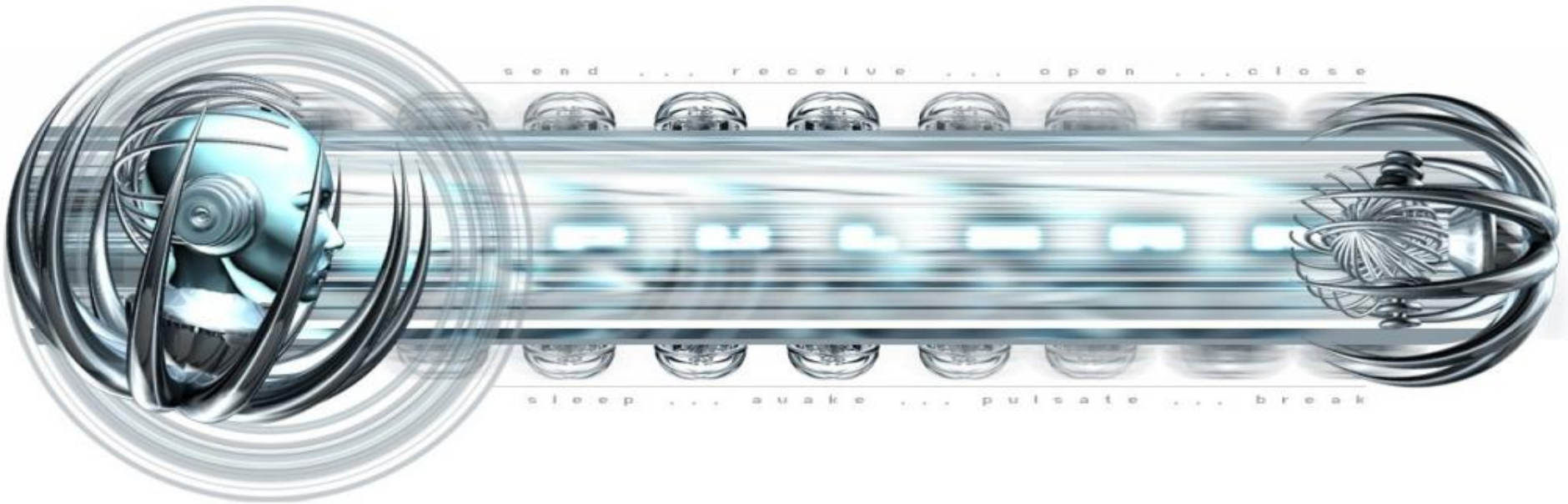
From private email with a former spook:

"Disclosing the method of attacking PGP would involve disclosing classified cryptographic analysis methods (I was taught by the government), and such a disclosure to uncleared persons would be seriously illegal (in wartime such a disclosure carries the death penalty).

Seriously though, I would love to lay out the holes in several crypto systems, and would love to disclose the methods for breaking PGP, DES, and a number of other civilian crypto system I have studied (in multiple NSA crypto schools); but will not disclose information and/or methods I know to be classified." and

"The fact that various world governments can perform a PGP decrypt is old news, and not classified, however; the exact method used for the decrypt is what is classified."

WHAT CAN SATAN SNIFF?



Other informal sources

TYPES OF MONITORING



retina reflector

<http://misery.subnet.at>

INVASIVE, NON-INVASIVE, STEALTH

TYPES OF MONITORING



retina reflector

<http://misery.subnet.at>

NON-INVASIVE - MONITORING NODES ARE OBVIOUS. LITTLE TO NO TRAFFIC IMPACT. USUALLY EASY TO AVOID.

TYPES OF MONITORING



retina reflector

<http://misery.subnet.at>

STEALTH - MONITORING NODES ARE NOT OBVIOUS. NO TRAFFIC IMPACT. HARD TO AVOID.

TYPES OF COMMUNICATION

The background features a dark blue gradient with a central horizontal band of bright, glowing blue light waves that resemble a signal or data stream. On the right side, there are complex, metallic, and reflective structures that look like stylized leaves or petals, rendered in shades of blue and silver.

POINT TO POINT (E.G. EMAIL)

BROADCAST (E.G. USENET)

TYPES OF COMMUNICATION

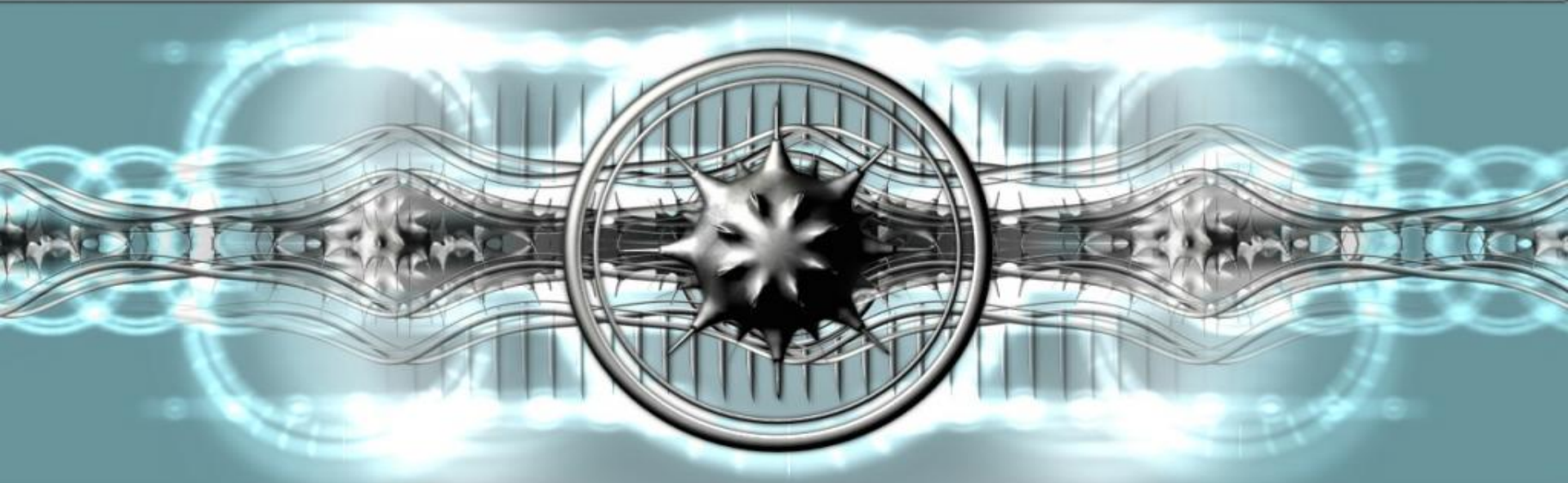
The background features a dark blue gradient with horizontal light trails in white and light blue, resembling data or signal paths. On the right side, there are complex, metallic, and reflective structures that look like stylized plants or mechanical parts, rendered in shades of grey and blue.

ANONYMOUS SENDER (E.G.
REMAILER)

TRAFFIC PATTERN MASKING (E.G.
LOKI)

To AVOID STEALTH MONITORING, STEALTH COMMUNICATIONS ARE NEEDED

REPLICATION - CREATION - DISINTEGRATION - DISILLUSION



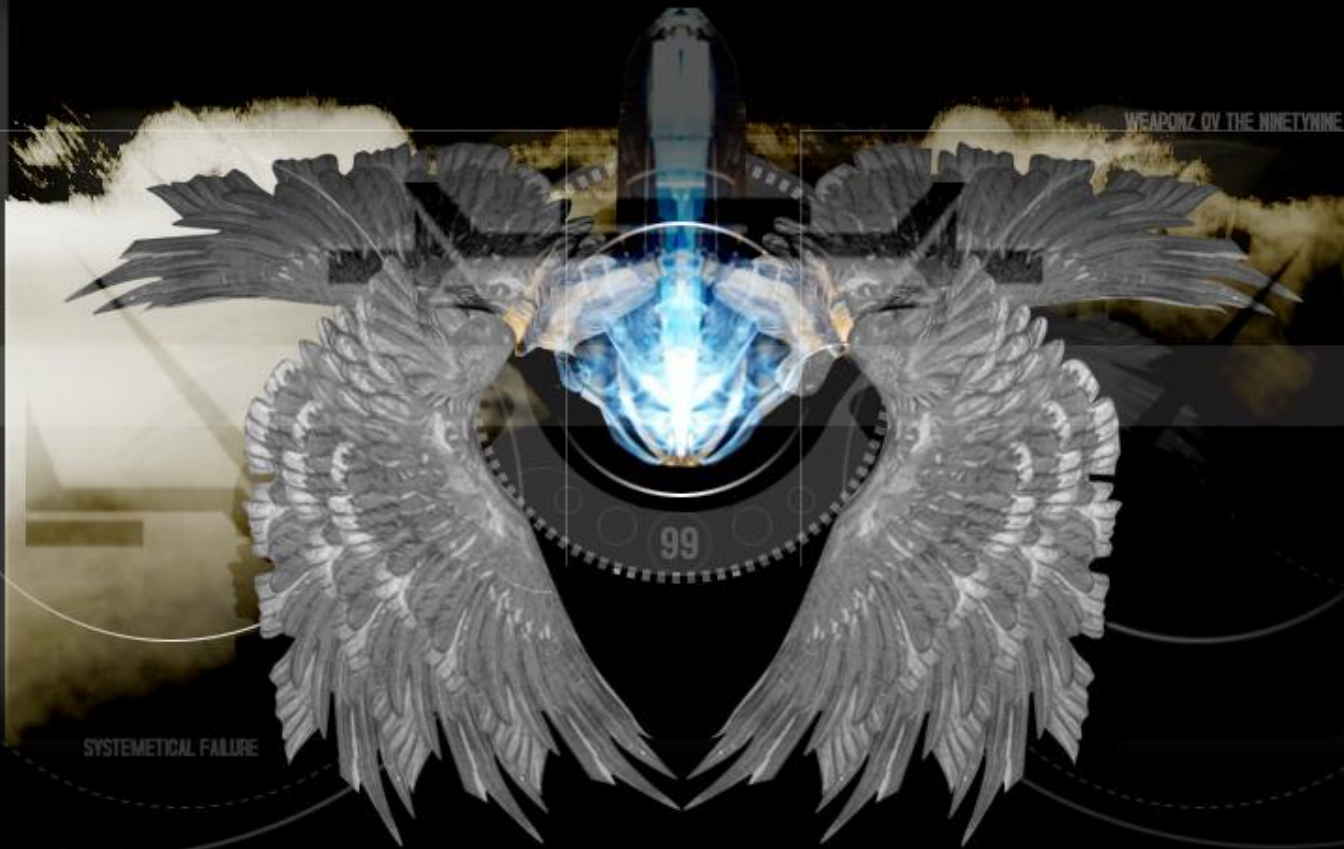
SUBDIRECTED - DISINFORMED - UNCONTROLLED - NEGOTIATED

STEALTH COMMUNICATIONS - SENDER/RECEIVER
UNKNOWN. MESSAGE ENCRYPTED.
COMMUNICATION NOT OBVIOUS, DIFFICULT TO
DISCERN FROM REGULAR TRAFFIC.



DIGITAL DROP BOX

SCENARIO # 1

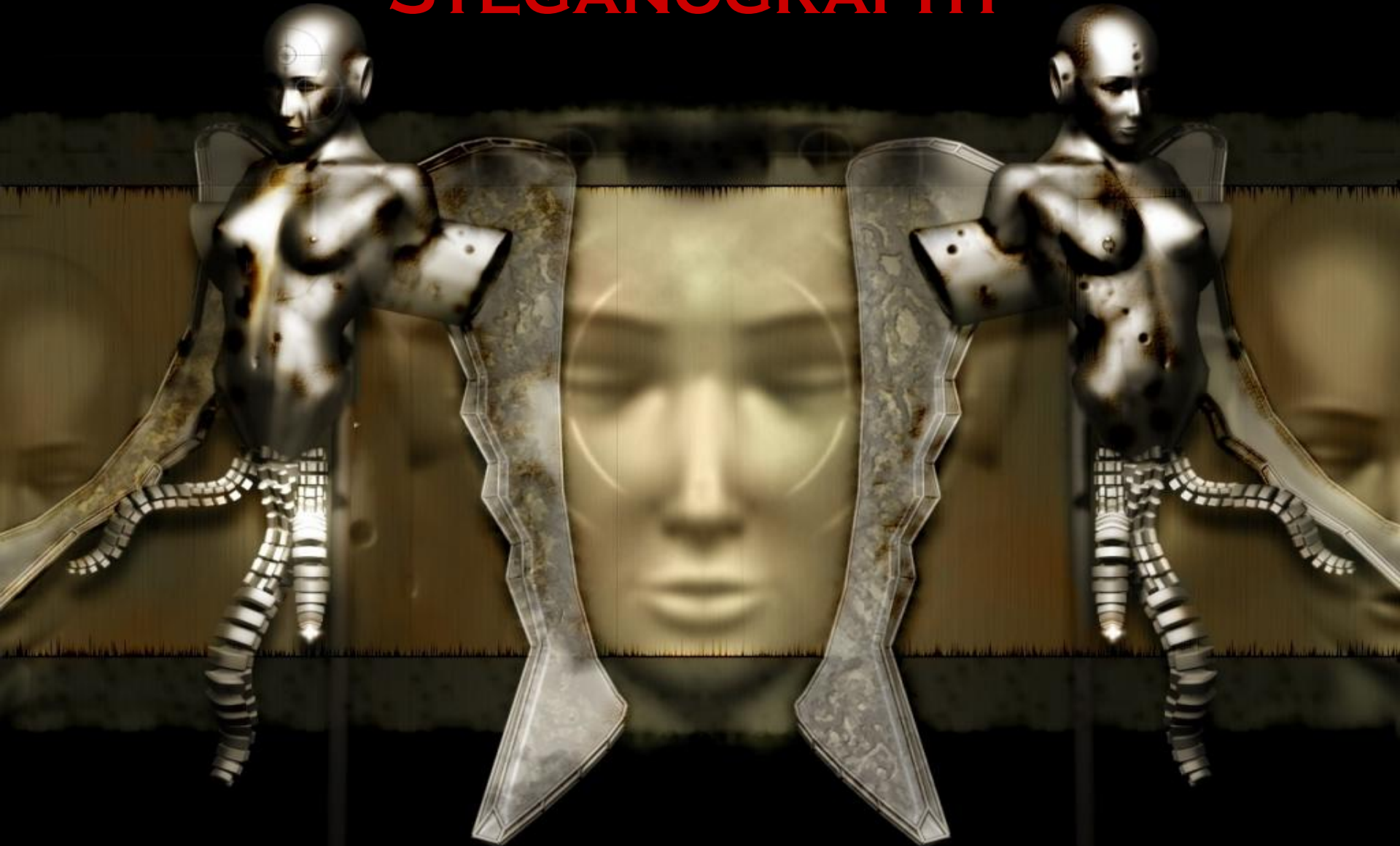


STEALTH DIGITAL DROP BOX USING HOLEPUNCH

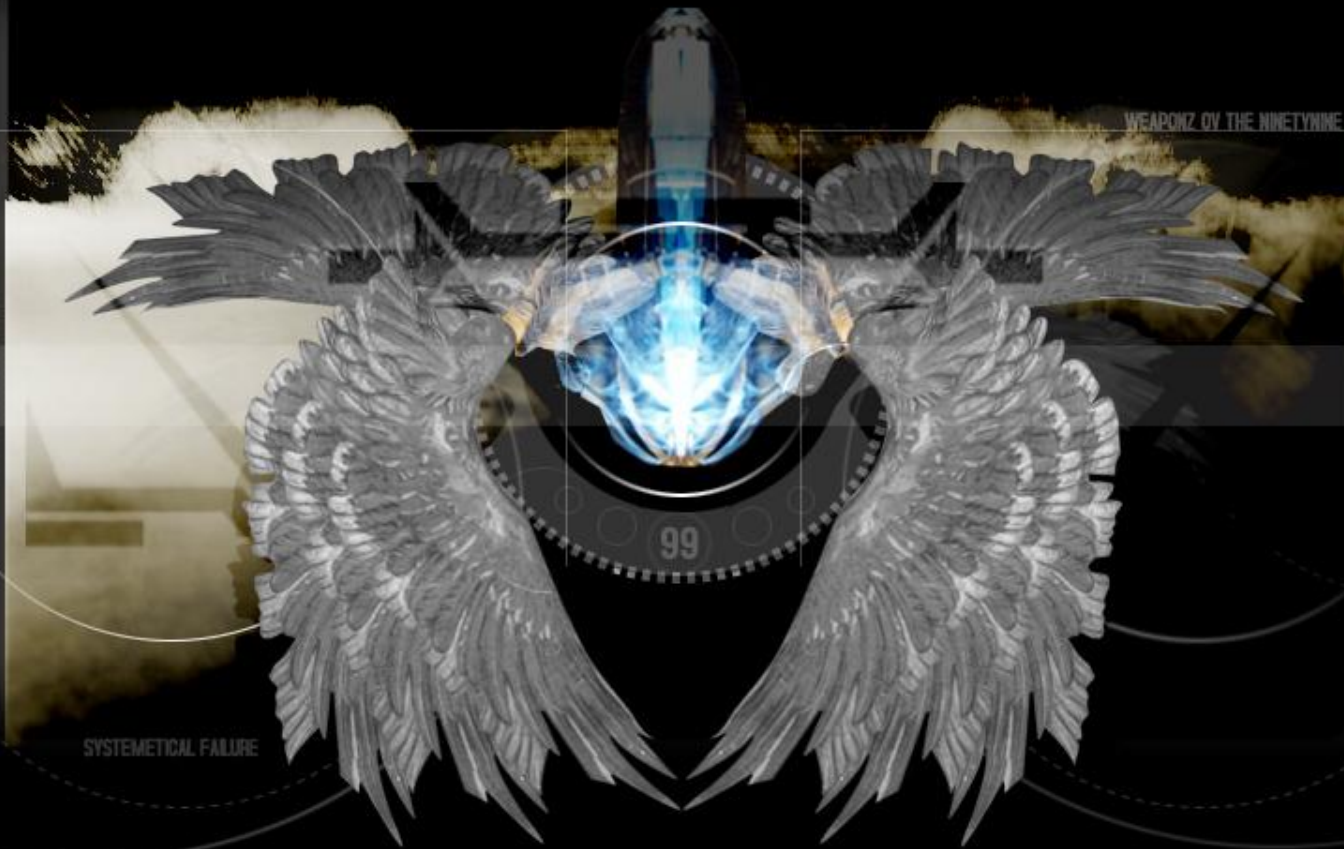
M1S*R3D ninetynine
D1S CO/RD #63



STEGANOGRAPHY



SCENARIO #2



STEGANOGRAPHY USING OUTGUESS AND PORN

M1S*R3D ninetynine
D1S CO/RD #63





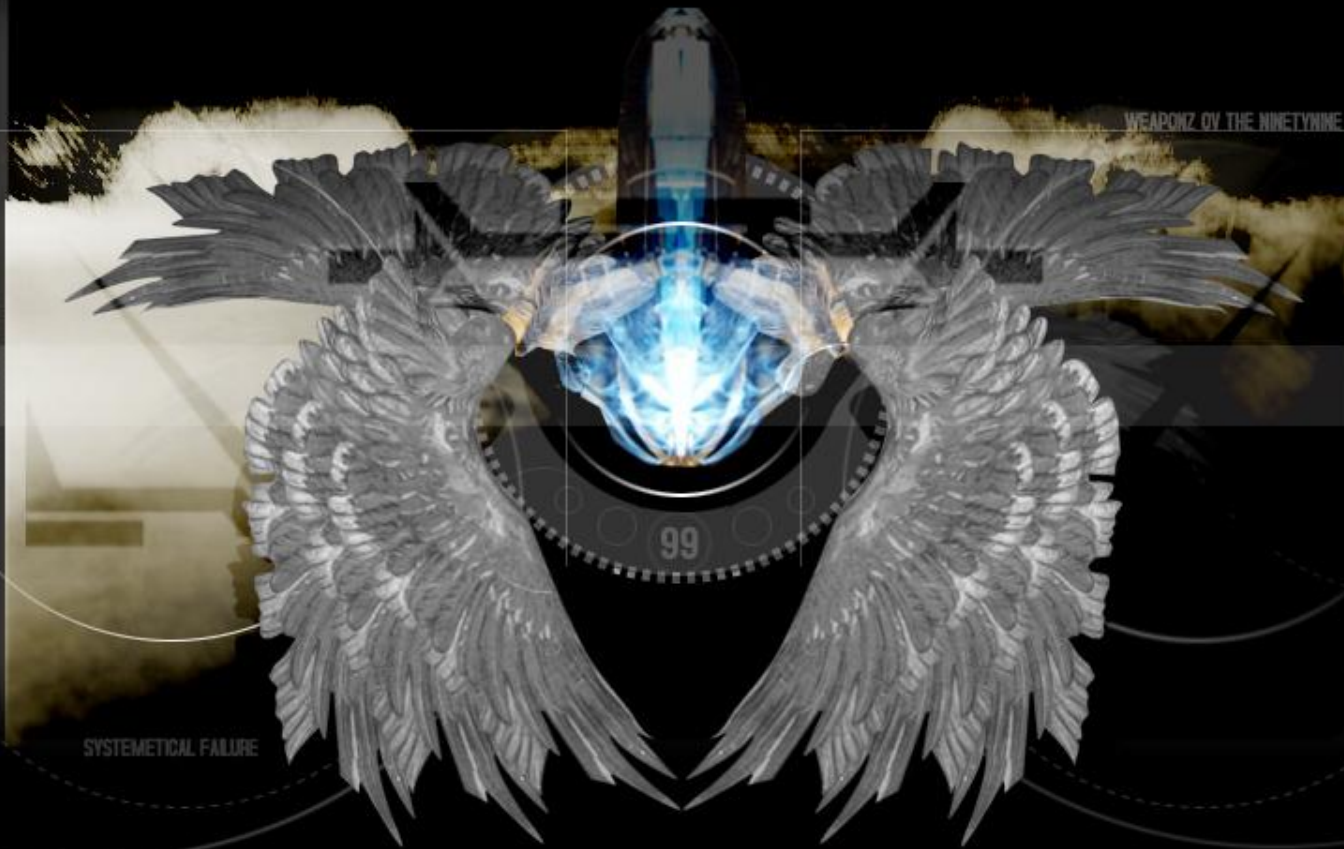
AND THE FOUR ST...
TO COME OUT
BU...

RETINA REFLECTOR II

STEALTH TRAFFIC PATTERN MASKING

lateral gesehen

SCENARIO #3



STEALTH TRAFFIC PATTERN MASKING USING
MASQUERADE

M1S*R3D ninety-nine

D1S CO/RD #63

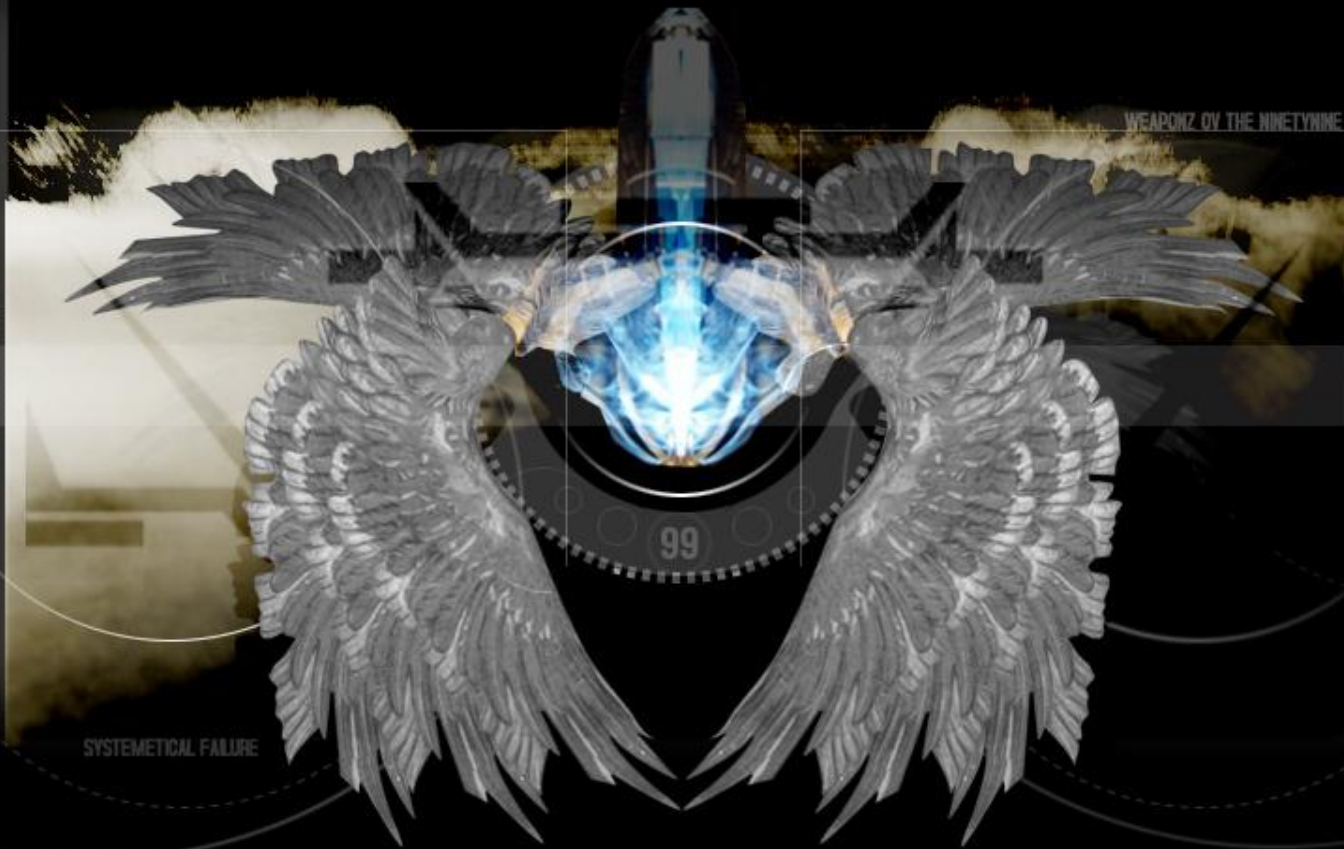


DINING CRYPTOGRAPHERS PROBLEM



Basics behind a DC Net
Scaling issues solved with CliqueNet

SCENARIO #4



ANONYMOUS POINT-TO-POINT COMMUNICATIONS
USING CLIQUENET

M1S*R3D ninetynine

D1S CO/RD #63



RETROACTIVE

FIN

QUESTIONS?

ALL QUESTIONS MUST BE IN THE FORM OF AN ANSWER

GRAPHICS FROM DEADDREAMER.COM