Don’t Fuck It Up!
Unjust laws exist: shall we be content to obey them, or shall we endeavor to amend them, and obey them until we have succeeded, or shall we transgress them at once?

—Henry David Thoreau, Civil Disobedience
Spy Eye v1.3

Encryption key (for config):
smthrandomkey

Clear cookies every startup (IE, FF):
Delete non-exportable certificates:
Don't send http-reports:

Compress build by UPX v3.07w:

Make build without ZLIB support
(SpyEye may use zlib for unpacking gzip or deflate content at FF webinjects ... so, this option can save 15-16 KB):

Make LITE-config
(without webinjests, plugins & screenshots):

• EXE name: Recycle.Bin

• Mutex name: SystemService

Make config & get build
Hands Off My Internet!

When you download internet porn, you're jerking off with Hitler!
"On the Internet, nobody knows you're a dog."
On the Internet, everyone knows you like ASCII Goatse.
New Collection Posture

- Sniff it All
  - Torus increases physical access

- Partner it All
  - Work with GCHQ, share with Misawa

- Know it All
  - Automated FORNSAT survey - DARKQUEST

- Collect it All
  - Increase volume of signals: ASPHALT/A-PLUS

- Exploit it All
  - Analysis of data at scale: ELEGANTCHAOS

- Process it All
  - Scale XKS and use MVR techniques
# Tradecraft

<table>
<thead>
<tr>
<th>Perceptual Biases</th>
<th>Biases In Evaluating Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expectations</td>
<td>Consistency</td>
</tr>
<tr>
<td>Resistance</td>
<td>Missing Information</td>
</tr>
<tr>
<td>Ambiguities</td>
<td>Discredited Evidence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biases In Estimating Probabilities</th>
<th>Biases In Perceiving Causality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Rationality</td>
</tr>
<tr>
<td>Anchoring</td>
<td>Attribution</td>
</tr>
<tr>
<td>Overconfidence</td>
<td></td>
</tr>
</tbody>
</table>
Tradecraft

- Key Assumptions Check
- Quality Of Information Check
- Contrarian Techniques
  - Devil’s Advocacy
  - High Impact/Low Probability
  - “What If?” Analysis
- Red Team
OPSEC

ENEMY EARS are listening
THE BOTTOM LINE ON OPSEC;

We all have information that the Bad Guys need to hurt us. We don't want them to get it. The OPSEC process helps us to look at our world through the eyes of an adversary and to develop measures in order to deny them. Get it?

The OPSEC Process:

1. Identify Critical Info
2. Analyze Threats
3. Analyze Vulnerabilities
4. Assess the Risks
5. Apply Countermeasures

WHAT IS OPERATIONS SECURITY?
Operations Security, or OPSEC, is a risk management methodology used to deny adversary information concerning our intentions and capabilities by identifying, controlling, and protecting critical information associated with the planning and execution of a mission.
The 7 Deadly Fuckups

- Overconfidence
- Trust
- Perceived Insignificance
- Guilt By Association
- Packet Origin
- Cleartext
- Documentation
WARNING

Keep hands away from jet.
Don’t Fuck It Up When You Use A VPN

- Traffic Encryption
- Location Obfuscation
- Request Concealment
  - ...Depending On Listener Location
  - ...Depending On Provider
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>158</td>
<td>50.727396000</td>
<td>10.1.10.233</td>
<td>224.0.1.76</td>
<td>IAPP</td>
<td>128</td>
<td>Announce Response(1) (version=1)</td>
</tr>
<tr>
<td>159</td>
<td>50.728072000</td>
<td>10.1.10.233</td>
<td>224.0.1.76</td>
<td>IAPP</td>
<td>128</td>
<td>Announce Response(1) (version=1)</td>
</tr>
<tr>
<td>161</td>
<td>51.617440000</td>
<td>10.1.10.15</td>
<td>224.0.0.251</td>
<td>MDNS</td>
<td>147</td>
<td>Standard query response 0x0000 TXT</td>
</tr>
<tr>
<td>162</td>
<td>51.779381000</td>
<td>10.1.10.12</td>
<td>224.0.0.251</td>
<td>MDNS</td>
<td>194</td>
<td>Standard query 0x0000 PTR_afpovertcp_.tcp.local, &quot;QM&quot; question PTR_smb.</td>
</tr>
<tr>
<td>159</td>
<td>52.668754000</td>
<td>10.1.10.15</td>
<td>224.0.0.251</td>
<td>MDNS</td>
<td>147</td>
<td>Standard query response 0x0000 TXT</td>
</tr>
<tr>
<td>166</td>
<td>53.788231000</td>
<td>10.1.10.34</td>
<td>10.1.1.255</td>
<td>BJNP</td>
<td>60</td>
<td>Scanner Command: Discover</td>
</tr>
<tr>
<td>167</td>
<td>53.788293000</td>
<td>10.1.10.34</td>
<td>224.0.0.1</td>
<td>BJNP</td>
<td>60</td>
<td>Scanner Command: Discover</td>
</tr>
<tr>
<td>172</td>
<td>54.575054000</td>
<td>10.1.10.34</td>
<td>224.0.0.251</td>
<td>MDNS</td>
<td>147</td>
<td>Standard query response 0x0000 TXT</td>
</tr>
<tr>
<td>201</td>
<td>60.879248000</td>
<td>10.1.10.34</td>
<td>10.1.1.255</td>
<td>BJNP</td>
<td>60</td>
<td>Scanner Command: Discover</td>
</tr>
<tr>
<td>202</td>
<td>60.879254000</td>
<td>10.1.10.34</td>
<td>224.0.0.1</td>
<td>BJNP</td>
<td>60</td>
<td>Scanner Command: Discover</td>
</tr>
<tr>
<td>206</td>
<td>67.975528000</td>
<td>10.1.10.34</td>
<td>10.1.1.255</td>
<td>BJNP</td>
<td>60</td>
<td>Scanner Command: Discover</td>
</tr>
<tr>
<td>207</td>
<td>67.975534000</td>
<td>10.1.10.34</td>
<td>224.0.0.1</td>
<td>BJNP</td>
<td>60</td>
<td>Scanner Command: Discover</td>
</tr>
<tr>
<td>218</td>
<td>73.904524000</td>
<td>10.1.10.34</td>
<td>255.255.255</td>
<td>DB-LSP-DI</td>
<td>156</td>
<td>Dropbox LAN sync Discovery Protocol</td>
</tr>
</tbody>
</table>

Frame 0: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Encapsulation type: Ethernet (1)
Arrival Time: Jul 15, 2014 16:38:29.084650000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1405456709.084650000 seconds
[Time delta from previous captured frame: 0.135622000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 4.134823000 seconds]
Frame Number: 6
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Coloring Rule Name: UDP]
Write failed: Permission denied
[Vomitose:~] zoz%

AnyConnect
Secure Mobility Client

VPN
The VPN connection has been disconnected due to the system suspending. The reconnect capability is disabled. A new connection is necessary, which requires re-authentication.

% killall -STOP Mail thunderbird Google Safari Firefox Adium Dropbox
% killall -CONT Mail thunderbird Google Safari Firefox Adium Dropbox

% cat /bin/rmac
#!/bin/csh -f

/System/Library/PrivateFrameworks/Apple80211.framework/Resources/airport -z
set rnd_mac_addr = 00:openssl rand -hex 51 sed 's/\(\.)\1:/g; s/.://'/
/sbin/ifconfig en1 ether $rnd_mac_addr
%
Technology Detection

- Show me all the VPN startups in country X, and give me the data so I can decrypt and discover the users

- These events are easily browsable in XKEYSCORE
  - No strong-selector

- XKEYSCORE extracts and stores authoring information for many major document types – can perform a retrospective survey to trace the document origin since metadata is typically kept for up to 30 days

- No other system performs this on raw unselected bulk traffic, data volumes prohibit forwarding
CES/SSC/AAD VPN “Surge”

• Main Goal:
  – To evaluate SCS VPN access and analysis to determine better methods of identifying and exploiting networks of interest.

• Two Focuses:
  – What can we do with VPN data that is already ingested into the system?
    • Find better methods of reporting VPN stats and exploitation determinations from CES back to SSC and site.
  – Are there methods to better identify and survey VPN’s to provide CES the data they need?
    • Can we leverage MIRROR, DARKQUEST, PANOPLY survey information to quickly identify and report the presence of VPN’s in surveyed signals?
    • Can we use BIRDWATCHER or other means to automatically resurvey for key exchanges and obtain paired collect?
SCS Opportunities

SCS PoPs provide opportunities for access, enabling, and analysis.
Private Networks are Important

- Many targets use private networks.

<table>
<thead>
<tr>
<th>Google infrastructure</th>
<th>SWIFT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>REDACTED</td>
<td>REDACTED</td>
</tr>
<tr>
<td>REDACTED</td>
<td>Gazprom</td>
</tr>
<tr>
<td>Aeroflot</td>
<td>REDACTED</td>
</tr>
<tr>
<td>French MFA</td>
<td>REDACTED</td>
</tr>
<tr>
<td>Warid Telecom</td>
<td>Petrobras</td>
</tr>
<tr>
<td>REDACTED</td>
<td>REDACTED</td>
</tr>
</tbody>
</table>

- Evidence in Survey: 30%-40% of traffic in BLACKPEARL has at least one endpoint private.
Remember:
PPTP Broken As Of
Don’t Fuck It Up When You Use Tor
Case Study: LulzSec/AntiSec
IRC WITHOUT TOR...

...NOT EVEN ONCE
Moral:

- Don’t Fail Unsafe With Tor
- Always Check What You’re Exposing
- OPSEC Is 24/7
Case Study: Harvard Bomb Hoax

Sorry, a system error occurred.

ID = 15
WHAT AIN’T NO COUNTRY I EVER HEARD OF

THEY SPEAK OPSEC IN WHAT?
What Fucked It Up?

- Harvard Network Registration
- Outgoing Traffic Logs
- Pervasive Surveillance Microcosm
- Moral:
  - Key Assumptions Check
  - High Impact/Low Probability Analysis
  - Bridge Relays
  - Traffic Analysis Preparation
(TS//SI//REL) Fingerprinting TOR

(TS//SI//REL) BuildID gives a timestamp for when the Firefox release was built

20121024073032
Year Month Day Hour Min Sec

(TS//SI//REL) tbb-firefox’s BuildID:

0

(TS//SI//REL) Exploiting TOR

- (TS//SI//REL) tbb-firefox is barebones
  - Flash is a no-no
  - NoScript addon pre-installed... but not enabled by default!
  - TOR explicitly advises against using any addons or extensions other than TorButton and NoScript
- (TS//SI//REL) Need a native Firefox exploit

(TS//SI//REL) Fingerprinting TOR

- (TS//SI//REL) TorButton cares about TOR users being indistinguishable from TOR users
- (TS//SI//REL) We only care about TOR users versus non-TOR users
- (TS//SI//REL) Thanks to TorButton, it’s easy!

(TS//SI//REL) Exploiting TOR

- (TS//SI//REL) ERRONEOUSINGENUITY
  - Commonly known as ERIN
  - First native Firefox exploit in a long time
  - Only works against 13.0-16.0.2
- (TS//SI//REL) EGOTISTICALGOAT
  - Commonly known as EGGO
  - Configured for 11.0-16.0.2...
  - ...but the vulnerability also exists in 10.0!
Tor Stinks...

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a very small fraction of Tor users, however, no success de-anonymizing a user in response to a TOPI request/on demand.

Analytics:
Goes Inta Goes Outta/Low Latency
Find possible alternative accounts for a target: look for connections to Tor, from the target’s suspected country, near time of target’s activity.
- Current: GCHQ has working version (QUICKANT). R has alpha tested NSA’s version. NSA’s version produced no obvious candidate selectors.
- Goal: Figure out if QUICKANT works, compare methodologies. Gathering data for additional tests of NSA’s version (consistent, random and heavy user)

Analysis: Cookie Leakage
Use cookies to identify Tor users when they are not using Tor
- Current: preliminary analysis shows that some cookies “survive” Tor use. Depends on how target is using Tor (Torbutton/Tor Browser Bundle clears out cookies).
- Goal: test with cookies associated with CT targets
  - Idea: what if we seeded cookies to a target?
  - Investigate Evercookie persistence

Exploitation: QUANTUM
- QUANTUM to degrade/deny/disrupt Tor access?
- QUANTUMCOOKIE – forces clients to divulge stored cookies.
(S//REL) Open Source Multi-Hop Networks

- (S//REL) Tor
- (S//REL) Very widely used worldwide
- (S//REL) Open Source
  - (S//REL) Active Development
  - (S//REL) Mitigates Threats
- (S//REL) Very Secure
- (S//REL) Low enough latency for most TCP use
- (S//REL) Still the King of high secure, low latency Internet Anonymity
  - (S//REL) There are no contenders for the throne in waiting
(S//REL) **Tor** Project and friends Recent Activity

- (S//REL) **Tails**: Complete Bootable OS on CD for anonymity – includes **Tor**
  - (S//REL) Adds Severe CNE misery to equation
  - (S//SI//REL) Has been discussed by CT targets
Global Variable for Tor foreign directory servers. Searching for potential Tor clients connecting to the Tor foreign directory servers on ports 80 and 443.

$stor_foreign_directory_ip = ip('193.23.244.244' or '194.109.206.212' or '86.59.21.38' or '213.115.239.118' or '212.112.245.170') and port ('80' or '443');

this variable contains the 3 Tor directory servers hosted in FVEY countries. Please do not update this variable with non-FVEY IPs. These are held in a separate variable called $stor_foreign_directory_ip. Goal is to find potential Tor clients connecting to the Tor directory servers.

$stor_fvey_directory_ip = ip('128.31.0.39' or '216.224.124.114' or '208.83.223.34') and port ('80' or '443');

The fingerprint identifies sessions visiting the Tor Project website from non-FVEY countries.

fingerprint('anonymizer/tor/torproject_visit')=http_host('www.torproject.org') and not(xff_cc('US' OR 'GB' OR 'CA' OR 'AU' OR 'NZ'));

These variables define terms and websites relating to the TAILS (The Amnesic Incognito Live System) software program, a comsec mechanism advocated by extremists on extremist forums.

$TAILS_terms=word('tails' or 'Amnesic Incognito Live System') and word('linux' or 'USB' or 'CD' or 'secure desktop' or 'IRC' or 'truecrypt' or 'tor');
$TAILS_websites=('tails.boum.org/') or ('linuxjournal.com/content/linux*');
Case Study: Silk Road/DPR

Silk Road
anonymous marketplace

Shop by category:
Cannabis(162)
Ecstasy(33)
Psychedelics(119)
Opioids(33)
Stimulants(56)
Dissociatives(6)
Other(199)

1 hit of LSD (blotter) $1.13
1/8 oz high quality cannabis $3.17

This hidden site has been seized by the Federal Bureau of Investigation, in conjunction with the IRS Criminal Investigation Division, ICE Homeland Security Investigations, and the Drug Enforcement Administration, in accordance with the United States District Court for the Eastern District of New York.
What Fucked It Up?
To identify all the responsible HS directories for a particular service by prior connection attempt. Thus, should the attacker be able to obtain the IDs of the hidden service and the fingerprint of the first responsible hidden service directory. The attacker then has access to key pairs so that SHA-1 hash of the public keys would be unique.

As mentioned in the background section, the list of hidden services is long and widely distributed. For instance, the Silk Road hidden service was shut down online black market for illegal drugs.

Table I shows the number of requests over the course of one day and the rate of requests over the course of one week. This table is one of the six hidden service directories of the discovered Tor botnet, the Silk Road hidden service, and the DuckDuckGo search engine.

Table II shows the number of requests over the course of one day and the rate of requests over the course of one week. This table is one of the six hidden service directories of the discovered Tor botnet, the Silk Road hidden service, and the DuckDuckGo search engine.

Figure 4. Hidden service descriptor request rate during one day.

Figure 6. Increase in the number of Guard nodes.
Technical Analysis: Hidden Services

What do we know about Hidden Services?

- **Current**: No effort by NSA, some DSD and GCHQ work on ONIONBREATH.
- **Goal**:
  - Harvest and enumerate .onion URLs
  - Identify similar HS based on referrer fields
  - Distinguish HS from normal Tor clients

Technical Analysis: torbservers.net

Investigate the Amazon AWS cloud instances of Tor servers. How are IPs allocated and reassigned once bandwidth limit is reached? Impact on RONIN’s ability to detect nodes?

- **Current**: GCHQ set up Tor nodes on the AWS cloud during REMATION II.
JTRIG tools and techniques

(Redirected from JTRIG CITD - Covert Internet Technical Development)

| **ALLIUM ARCH** | JTRIG UIA via the Tor network. | OPERATIONAL | JTRIG Infrastructure Team |
| **ASTRAL PROJECTION** | Remote GSM secure covert internet proxy using TOR hidden services. | OPERATIONAL | JTRIG Infrastructure Team |
| **FRUIT BOWL** | CERBERUS UIA Replacement and new tools infrastructure – Primary Domain for Generic User/Tools Access and TOR split into 3 sub-systems. | DESIGN | JTRIG Infrastructure Team |
| **NUT ALLERGY** | JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system | PILOT | JTRIG Infrastructure Team |
| **BUMBLEBEE DANCE** | JTRIG Operational VM/TOR architecture | OPERATIONAL | JTRIG Infrastructure Team |
| **SILVER SPECTER** | Allows batch Nmap scanning over TOR | | JTRIG Software Developers |
| **SHADOWCAT** | End-to-End encrypted access to a VPS over SSH using the TOR network | | JTRIG OSO |
Don’t Fuck It Up When You Use The Phone

• How Does Your Phone Betray You? Let Me Count The Ways...
  • Metadata
  • Location
  • Contacts
  • Networks
  • Unique Identifiers
  • Cookies
  • Searches
  • Weak Crypto
  • Repeated Access
  • Autoconnect (Pineapple’s BFF)
  • Apps
  • Pattern Of Life
### Example of Current Volumes and Limits

![Graph showing current volumes and limits](image)

### Dupe Methodology

Compare records within various time windows that share identical selectors and locations, specifically:

- **LAC**
- **CellID**
- **VLR**
- **DesigChannelID**
- **IMEI**
- **ESN**
- **IMSI**
- **MIN**
- **TMSI**
- **MDN**
- **CLI**
- **ODN**
- **MSISDN**
- **RegFMID**
- **CdFMID**
- **CgFMID**
- **RegGID**
- **CdGID**
- **RegIID**
- **Kc**
- **CdIID**
- **CgIID**
- **MSRN**
- **Rand**
- **Sres**
- **Opcode**
- **RQ1**
- **XR1**
- **Q_CK1**
- **Q_IK1**
- **AU1**
- **NewPTMSI**
- **OSME**
- **DSME**
- **RTMSI**
- **PDP_Address**
- **TEID**
- **TLLI**
- **PTMSI**
- **PDDG**
Perfect Scenario – Target uploading photo to a social media site taken with a mobile device.

What can we get?

User Activity Leads

- Examine settings of phone as well as service providers for geo-location; specific to a certain region
- Networks connected
- Websites visited
- Buddy Lists
- Documents Downloaded
- Encryption used and supported
- User Agents

Targeting

Targeting both Telephony and DNI systems
- Call Logs
- SMS
- SIM Card Leads
- Email address
- IMEI/IMSI
- Unique Identifiers
- Blackberry PINS
Case Study: CIA/Abu Omar
OCD OPSEC:
Using A Burner Phone Without Fucking It Up

- **DO:**
  - Advance Purchase
  - Register Far Away
  - Lie To Phone Companies
  - Stay Dumb
  - Remove Battery
  - Fake Contacts
  - Minimize Use
  - Move & Switch
  - Falsify Call Network
  - Purpose Equipment
  - Thou Shalt Always Kill
OCD OPSEC:
Using A Burner Phone Without Fucking It Up

- DON’T EVER:
  - Co-Localize
  - Co-Activate
  - Co-Contact
  - Store Real Data
  - Match Entry/Exit
  - Bridge Online Metadata
Don’t Fuck It Up When You Use Messaging

- After All These Years, E-Mail Still Sucks
- Spam Fighting Aids Tracking
- Webmail Using HTTP
- Weak Server-Side Storage
- Encrypted Content Not Metadata
- Insecure Client-Side Logging
- Bad Retention Habits
- Google
- And IM Is Not Much Better
- Psycho Ex Principle
SECURITY BY OBSCURITY DOESN'T WORK

TELL THAT TO THESE GUYS
Case Study: CIA/Petraeus
What Fucked It Up?

- Technique Already Identified & Compromised
- Pervasive Surveillance Designed ToExpose Exactly This Type Of Access Correlation
- Deleted Things Aren’t
- Understand & Manage Insecure Channels
  - Quality Of Information Check, “What If?”
Common Broken/Compromised Services

- Commercial Webmail
- Run Your Own Mailserver
- Metadata’s Still A Bitch
Common Broken/Compromised Services

- Skype
- PRISM, SIGINT Enabling, JTRIG, Forced “Upgrades”, Pre-MS EOL
- Fuck Skype
Common Broken/Compromised Services

Why are we interested in HTTP?

- Almost all web-browsing uses HTTP:
  - Internet surfing
  - Webmail (Yahoo/Hotmail/Gmail/etc.)
  - OSN (Facebook/MySpace/etc.)
  - Internet Searching (Google/Bing/etc.)
  - Online Mapping (Google Maps/Mapquest/etc.)

XKS HTTP Activity Search

Another common query is analysts who want to see all traffic from a given IP address (or IP addresses) to a specific website.

- Many Chats
  - Let’s Just Assume IRC Is All Collected
  - Why Not Grab 6667 Like 80?
  - TLS Only Protects You To The Server
  - QUANTUMBOT
  - GChat’s “Off The Record” Isn’t The Same As OTR
  - That First OTR Message
What Might Not Be Completely Fucked

- Some OTR Implementations (But Which Ones?)
- Cryptocat?
- Bitmessage?
- Retroshare?
- We Need More:
  - Auditing
  - Steganography
So what if I’m a glasshole? You are too.
Steganography: Hiding In Plain Sight

(U) Analytics for Targets in Europe

- (C//FVEY) OPSEC Savvy Targets
  - “…most terrorists stop thru Europe”
- (TS//FVEY) Use advanced techniques
  - Steganography
    - Forensics or Analytics on front end
  - Encryption
    - Takes time and has “black hole” issue
- (TS//SI//FVEY) Reliance on “special” collection
  - GCHQ and FAA
  - Problems processing w/r to TS
Steganography: Hiding In Plain Sight

- **Reported But Docs Not Released:**
  - P2P Traffic High Volume/Low Value
  - GCHQ TEMPORA Minimizes, 30% Ingest Reduction
  - Need To Hide In This Flood
Unfortunately, there are issues with undesirable images within the data. It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream without necessarily sending a reciprocal stream means that it appears sometimes to be used for broadcasting pornography.

A survey was conducted, taking a single image from each of 323 user ids. 23 (7.1%) of those images contained undesirable nudity. From this we can infer that the true proportion of undesirable images in Yahoo webcam is 7.1% ± 3.7% with confidence 95%.

**[edit] Potentially Undesirable Images**

We use face detection to try to censor material which may be offensive but this does not work perfectly so you should read the following before using OPTIC NERVE:

- It is possible to handle and display undesirable images. There is no perfect ability to censor material which may be offensive. Users who may feel uncomfortable about such material are advised not to open them.
- You are reminded that under GCHQ's offensive material policy, the dissemination of offensive material is a disciplinary offence.
- Retrieval of or reference to such material should be avoided; see IB 150 for guidance on dealing with offensive material.
H4x0rz: Lose The Ego

- Burner Rules For IDs
- IRL Identity Real And Separate
- Know & Compartementalize Pseudonyms
- Cred Is Another Enemy
- Really Burn Them, No Really
Don’t Fuck It Up, And After You Do:

- Contingency Planning
- Plausible Deniability
- Adversary Capability
- Seek Advice In Advance
- Support Those Who Provide It
- Good Luck & Never Surrender To Obedience
Stylometrics: Don’t Fuck It Up

- Resist Providing A Corpus
- Obfuscate
  - Machine Translate
- Imitate
- Alpha Tools: JStylo/Anonymouth