**Establishing Cover**

**Setting up your environment and identities**

**Will separate security domains per identity**

**A cover**

* A character or identity that will appear to be responsible for your actions
* This person will take the heat

Establish fake twitter, facebook, reddit etc. for private activities in the future

Fakenamegenerator.com

* Use a manager like lastpass to store information on each alias
* Will give you the information that you may need for a separate alias, it isn’t just a name

Must use the same VPN or VM to access those aliases

Create an entire person that you can EMBODY so that you never accidentally provide profiling information related to your real ID

* Even talking about the weather in your area is enough to locate you

When you’re in character, become the character and never fall out of it

Research everything about the alias so that you can keep it up and not slip up

* You better speak Russian if your alias is Russian
* Have to treat this like method acting
* Create a whole history and present

**Sub alias**

Say you are a political dissident, you may sign up to a forum with a username that doesn’t relate to your alias

But the email you use is connected to the alias

At least this means that if any investigation is carried out on the forums, then the user will be traced back to the alias and not you

**Proper Planning and Practice, Prevents Piss Poor Performance**

One mistake in timing, configuration and planning can be enough to blow cover

* Practice creating aliases and use them for legitimate purposes to get to grips with it
* After a while, determine whether you have been successful, was there any contamination?
* Only when you have reached a professional level, should you then use aliases for other things
* Once an alias has been used for its purpose, its time to consider retiring it
* The more interactions the alias has, the more risk is associated with it

**The real world**

At the highest level, online anonymity means that you have to be anonymous offline as well without any compromises

You cannot guarantee total anonymity online even when using encryption, Tor, Gateways, VPNs, Virtual Machines

* Unless you are anonymous in the real world, an adversary can track you still

‘The Baby Harvest’ – how birth certificates and registration is moving online

DEF CON, Chris Rock – I will kill you

* The ability to actually register a new ‘fake’ real world identity
* Fake IDs and fake real-life aliases on Dark Web

**Identity Cross-Contamination**

Layers of isolation and compartmentalisation help reduce ID cross-contamination

* No contact between IDs and aliases
* Spend time searching for cross contamination between aliases
  + Start with google searches
  + Obviously using anonymising services to do this

If there are any contaminations, either get rid of them or cut your losses completely

* If the tree is poisoned, don’t keep eating the fruit

Cnet – how to delete yourself from the internet

Google – remove their stored data on you

Most social media allow you to delete your accounts but is highly likely that they have archive back-ups of the data

For accounts that cant be deleted, falsify the accounts

* Post fake information
* Change the name, change cities, change gender etc

Unsubscribe form mailing lists

Delete search engine history

Contact webmasters and people that run the websites to delete content

Get unlisted with phone companies

Delete email

Edit posts or delete them

Waybackmacine.org

* Internet archives
* Your posts from the past will be archived by sites like this
* The archives can be deleted if you contact them – [info@archive.org](mailto:info@archive.org)

The right to be forgotten