g23

Operational **Sec**urity

version 0.1 April 2016

page intentionally left blank

- Theory
  - Definition
  - Principles
  - Flow
  - OpSec process
  - Need to X – Principle
  - Atomicity
- Methods
  - Classification, Compartmentalization, Separation, Isolation
  - Accounting
  - Reporting & Alerting
- Application
  - Prevention Checklist - again
  - General Rules
  - Notes
    - Shut up
    - Baseline
    - Cover & Legend
    - Pocket litter – cars, bikes, bags and trackers. Cleanup
    - Paper destruction
    - Biotraces
    - Deniable physical communication
    - Wifi security
    - Cellphone security
    - Calling and phone concentrators
    - Travel security
    - Be early, leave late
    - Travel to/from meetings
    - Air-travel
    - Secure room (hotel or home)
    - Signals, Alarms, Fallbacks
    - Caches (physical and digital)
    - Temporary caches, lockers
    - Bug-out bag, EDC
    - Payments
    - Air gap computers
    - Dead Drops
    - Brushes
    - Rally Points
  - End notes, Twelve Commandments

Theory: Definition

OpSec is the control of information- and artifact-flow that could endanger operational success or operational capabilities. It is a default position that does not rely on opponent interaction (as does offensive counter-intelligence).

Theory: Principles

Deterrence by opponent:

- **Acceptability:** Is the behavior unacceptable to the opponent? If yes, the opponent will spend resources to detect, deceive and/or neutralize.
- **Credibility:** Can the opponent gather intelligence that makes the threat credible and demonstrable? Is there evidence or cause for reasonable suspicion.
- **Perception:** Does the opponent see/know information relating to operations, assets, capabilities and persons?

Detection by opponent:

- **Who is involved?** Names, aliases, skills, background, identifying marks (biometric, technological, habitual).
- **What is done?** Operation.
- **How is it done?** Methods, resources, technology, tools.
- **When is it done?** Time, date, event relations (eg. after conference, two days after meeting).
- **Where is it done?** Address, place, geolocation, place relation (eg. restaurant within 5 minutes walking distance to hotel).
- **Where is an asset?** Person or resource. Address, place, geolocation, place relation (same city as another asset).
- **With whom or what is a person/asset related?** Ownership / possession of resources, social relationships, affiliations.
- **Why is something done?** Goals, motives, assumptions of effectiveness.
- **Gaining access:** Documents, information, keys, passwords, identifiers, tools, decoration, etc.

Opponent will use criminology, forensics and various collection methods. The opponent does not require certainty but usually operates on likelihood/probabilities and alternative explanations.

Some opponents have an **unlimited and long-time memory.**

Counteraction by opponent:

- **Deception** to direct target action towards opponent's goals.
- **Implants** to stabilize access. Technologies, methods, artifacts, persons, cars, other assets.
- **Offensive capture** to increase information, asset or person outflow.
- **Neutralization** to prevent operative success to the target or dismantle/destroy the target. Destroy assets or permanently undermine trust, reliability or confidentiality.

Counteraction by target:

- **Cover:** Increase perceived acceptability by opponent to decrease opponent motivation.
- **Deception, camouflage, decoy:** Decrease credibility in the eyes of opponent or misdirect concerning operational goals. Conceal capabilities, assets and skills. Use of short operations and small organizations. Display intentional error.
- **Conceal:** Reduce perception and detection.
- **Detection:** Identify and insulate implants. Prevent implants of possible.

The goal is to **prevent neutralization and manipulation** by the opponent.

Theory: Flow

Object type	Flow direction	Opponent Principle	Effect
Information	T => O	Perception	Offensive capture, Implants
Artifact	T => O	Credibility	Neutralization
Person	T => O	Perception, Credibility	Offensive capture, Neutralization
Information	O => T	Deception	Neutralization
Artifacts	O => T	Deception	Offensive Capture, Neutralization
Persons	O => T	Deception, Credibility, Perception	Offensive Capture, Deception, Neutralization, Implants

T => O: Target to opponent **O => T**: Opponent to target

Theory: OpSec process

Prevent, Prepare, Respond, Recover

- **Prevent:** Control asset/artifact/information flows. Limit information content of artifacts/documents/conversations. Limit information lifetime/relevance. Limit predictability. Prevent and/or limit impact of outflow/leak.
- **Prepare:** What happens in case of outflow/leak? How to contain leaks? How to do damage assessment? Fail-over/emergency plans. Emergency/Danger signals. Detection methods. Protocols for containment, reporting. Backups and caches. Savings. Define rally points and side channels.
- **Respond:** Contain leak/implant. Destroy asset/artifact. Destroy ties/relationships/tracebacks. Notify necessary parties. Enact fail-over/emergency plans.
- **Recover:** Replace capabilities, assets, persons. Use side channels. Rally points. Access caches/backups.

Theory: Need to X – Principle

Need to **know,** need to **be there,** need to **be known**. The best prevention is limitation!

Only need justifies sharing, without need it is a critical mistake.

- (Who/What) needs to know (who/what)?
- (Who/What) needs to be there?
- (Who/What) needs to be known by others, at all?

Theory: Atomicity

Atomicity: By default nobody knows anything, is no where, knows nobody else, has no history or future. Sub Rosa/Secrecy is the default.

Cooperation and interaction destroys atomicity. The purpose of “need to X” is to **preserve atomicity** as much as possible while accomplishing the **minimal operational goal**.

Methods: Classification, Compartmentalization, Separation, Isolation

- **Classification:**
  - **Person:** Trustworthiness, reliability, integrity, skills, risk environment.
  - **Asset/Artifacts:** Security, reliability, usefulness, traceability, identifiability, impact/reach in case of capture.
  - **Information:** Impact/reach in case of capture. Necessity. Minimalism.
- **Compartmentalization:** Minimal persons, assets, information to accomplish a goal/task. Only necessity – nothing else.
- **Separation:** Each person has minimal access to play his part – nothing else. No reuse of assets/artifacts/methods if possible. Create minimal, simple viable tasks.
- **Isolation:** Each asset/artifact/information is only related to the absolute minimum number of other persons/assets/artifacts. Places/storage should not share unrelated artifacts/information.

Compartmentalization insulates operations. Separation insulates actions. Isolation insulates relationships and persons.

Classification enables selection of persons/assets for information sharing, task delegation and artifact possession.

Together, Compartmentalization, Separation and Isolation try to **preserve atomicity** as much as possible while accomplishing the **minimal operational goal** through the application of the “Need to X” principle.

Methods: Accounting

Keeping track of:

- Who knows what?
- Who possesses/has access to what?
- Who knows whom?
- Who/what is related to each other?
- Is involved in which operation/task?
- Date of and reason for entry

Accounting enables “Need to X” application by being able to determine the **operational footprint**.

Strict accounting and planning also increases the efficiency of response and recovery measures like caches, backups, signaling/notification and emergency savings. Without accounting it becomes impossible to assess the impact of compromises, breaches and leaks.

The method of accounting and the storage of this data needs special attention. Since the data relates to multiple operational contexts, persons, artifacts etc. accounting itself breaks all the need-to-X principles. This makes accounting data the treasure of any opponent. Extreme measures must be taken whenever accounting data is accessed, manipulated and stored. Use of strong encryption, dead man encryption, multi-party/four-eyes access, concealment/steganography, air-gapped computing and on-person carry at all times is prudent. It is also necessary to develop a quick, always executable and effective destruction method.

Methods: Reporting & Alerting

Accounting should include feedback so it can be effective in detection of problems, responding to attacks/leaks and recovering from failure.

Alerting: Communicate unusual and/or threatening/dangerous activities.

Reporting: Contacts, usage of assets/artifacts, shared information, learning.

Only with accounting, reporting and alerting can competition turn into **adaptive competition.**

Application: Prevention Checklist - again

. **First order:** Persons → Names, aliases, background, identifying marks. Addresses/locations of persons.

. **Second order:** Means of access → Keys, passwords, identifiers.

. **Third order:** Activities → Operations, Methods.

. **Fourth order:** Persons → Social relationships, affiliations, social graph.

. **Fifth order:** Places → Addresses, locations, locational relationships.

. **Sixth order:** Time → Dates/Time of activities, time relationships.

. **Sevenths order:** Goals, motives, ideology.

The higher the order, the more protection the item deserves and the more careful should any sharing be considered.

Application: General Rules

- Atomicity is the default.
- Everything (no exception) is a secret. Unless necessity says otherwise.
- Everything leaves a trace.
- Somebody or something is always watching or collecting.
- Need to know / be there / be known.
- DO NOT TALK.
- Outflow is a problem, inflow as well.
- OpSec should expose opponent actions. (Detection and Accounting)
- Reduce perception by opponent.
- Don't expose your social network. Don't drop names. Don't share contact details.
- Beware of traces, taps, trackers, storage, hidden information.
- Less data, less action means more security.
- Reconnaissance before action.
- Cooperate or conceal.

- Sharing is a threat.
- Keeping your mess around leads to big troubles. Delete/destroy what you don't need.
- Beware of garbage/pocket-litter. Clean up (bring under conscious control).
- Variation and randomization.
- Higher security through less efficiency → efficiency leads to repetition and sharing.
- Change operational footprint and signature.
- Create cover activities and habits to hide in the baseline.
- Reduce linkability → Many names, many legends.
- Beware of identifiers → social media, phones, numbers, addresses, photos, number plates, names, brands….
- Learn about opponent resources, methods, tactics. Be aware of manipulation and the unknown when relying on outside information.
- You connect everything: Keep security as high as the highest risk.
- Stay away from surveillance (cameras, crowds, automatic number plate recognition, cellphones, wifi hotspots….).
- Use imprecise/fuzzy information where information sharing cannot be avoided but is not necessary for operational success. (Social situations).
- Synchronize fuzzy information. It's a legend.
- Legends, covers. Give reason and satisfy want.
- Use your imagination.

OpSec is a lifestyle. Retain your operational capabilities in an age of mass data production and retention, surveillance states, corporate manipulators, intelligence competition (corporations as well), and noisy "transparent" societies.

Application: Notes

The following are notes, starting points for your own thinking. This is what is often called “defensive, pro-active” tradecraft. These notes are far from exhaustive, they are meant as inspiration and everyday practical advice. All digital OpSec has been excluded and will be covered by another seminar.

Application: Notes: Shut up

This is an remains rule number one. Do not talk about anything on the prevention checklist unless necessary, and unless ALL receiving parties have a need to know.

This is counterintuitive for post-moderns that use peer approval as a decision making method. It is fatal in security relevant situations.

Application: Notes: Baseline

The baseline is what is perceived as “normal” behavior/clothing. It applies both to the environment of a person and the person itself. Going “operational” should not change behavior in a way that deviates from the baseline. Behaviors that are adopted or dropped due to operational activity are strong signals to opponents.

For this reason the individual baseline should include behaviors that would be adopted during operations and it should not include behaviors that are dropped during operations. This includes cover activities that can be used in operations, like frequent and extended walks, going to cafes, default use of secure communications, payment with cash etc.

Application: Notes: Cover & Legend

All operational activities need to be supported by a reason that can be given for that behavior that does not reveal operational intentions. **Cover**s are these “good reasons” to be somewhere or do something that can be given as an explanation to a third party. Covers also include supporting documentation, knowledge, contacts, “pocket litter”, business cards etc.

Covers, especially if they include aliases/pseudonyms, are supported by a **legend** that spans biographical back story, anecdotes, contacts, employment situation/history. Legends should be verifiable - for example if an opponent searches the Internet, calls employers or neighbors. Verification should be controllable by the operative and allow for detection of verification. These controlled points of verification are called **backstops** and both put the opponent at easy and inform the operative about the ongoing background check – which can serve as a signal to retreat.

Application: Notes: Pocket litter – cars, bikes, bags and trackers. Cleanup

Every person carries many things without being aware of them. For example, the litter we carry in our pockets and wallets – receipts, boarding passes, business cards, tickets etc – paint a substantial picture of our activities and whereabouts.

It is also very easy to attach a tracker device to a car or bike, or slip it into a bag. Trackers are cheap and effective, making them ideal devices for cost efficient surveillance.

To prevent both problems it is important to regularly search pockets, bags and vehicles to get rid of trackers and litter. This should be done before each meeting/activity and after, before entering or leaving the area of operation.

In general no vehicles should be brought into operational areas or to meetings if at all possible. This also prevents an opponent from recording license plates around points of interest to identify persons of interest and assets.

Computers carry pocket litter as well!

CLEAN UP: Bags, bikes, cars, wallets, pocket, computers.

Application: Notes: Paper destruction

Using a “shredder” or burning alone does not help. For any kind of destruction (paper or other) the process must be attended from beginning to end, the remains verified.

An effective way to destroy paper is to burn the pages one by one, then grind down the ashes and flush the dust. No pieces larger then two square millimeters should be allowed to remain. Only burning paper is risky since burned pages still stick together and allow for reconstruction.

Application: Notes: Biotraces

Humans leave biological traces all the time. Fingerprints and DNA mostly. Mixed DNA sources are less of a problem because opponents cannot make easy use of them. However, defined (single person) DNA sources are easy to collect and archive.

In general, one should be careful of where and when to leave traces. Fingerprints in particular are easy to prevent using gloves or spray-on adhesive patches (available in pharmacies).

Especially when handling incrementing artifacts and documents care should be taken throughout the whole process.

Application: Notes: Deniable physical communication

When information needs to be exchanged in a meeting that might be under surveillance and/or the other party might be untrustworthy and trying to collect artifacts (evidence), the following protocol can be used:

- Do not vocalize incriminating information.
- Instead, write the information on a piece of paper, in block letters. If possible, do not write with your dominant/writing hand which is doable with a bit of practice and for block letters and short notices.
- If possible, cover your writing with the other hand.
- Use a hard, ideally glass, underground to write, and only use a single sheet.
- Mark the paper with a random, hard to (quickly) replicate pattern.
- Tear the paper so that part of the pattern is present on each piece.
- Fold the piece so that the message is not visible.
- Hand the message to the other party who should conceal it with his hands when reading.
- The other party has to return the message immediately after reading.
- Verify the pattern with your piece.
- Destroy both pieces immediately (burn and grind).

Application: Notes: Wifi security

Wifi/WLAN Ethernet and Bluetooth devices have unique identifiers that are publicly visible when used. Furthermore they reveal previous connection settings. To prevent both, each cover should come with its own set of devices or at least addresses.

As all cover-related devices/information they should be handled with care, used only during operation, and being disposed off as soon as possible. Storage should happen separate from other covers.

Application: Notes: Cellphone security

Cellphones are easy to track by almost anybody. Furthermore they carry a lot of sensitive information, and smart phones can also be turned into audio and video bugs.

In general, the use of cellphones is to be avoided. If they need to be used, the following rules apply:

- Never bring them into operational areas or to meetings. Leave them at home/hotel, switched on, and protected by a pass code/PIN. Switching them off/on during operation sticks out of the baseline and reveals sensitive information.
- Call logs, texts/short messages and contact/phone book should be cleaned up frequently, especially before and after operations.
- If possible, cellphones should be single-use. Destroy and dispose of them after use as soon as possible.
- Use different cellphones for different social graphs. Due to the tracking problem of phones this makes it necessary to only use phones that are not linked to ones name, and that are always physically separate from each other.
- Make calls, do not send short messages/texts. Texts are much easier to capture both from the phone as from the air, and their contents are recorded automatically.
- A rule never to break is: Do NOT bring the cellphone anywhere closer than 30 miles to the operational area (the GHCQ rule).

Best is to have a cellphone (like everybody else), but keep it at home, switched on, never carry it around.

Application: Notes: Calling and phone concentrators

Call patterns reveal social graphs. Especially in operational situations members of a team should never directly call each other. Instead they should call proxies that forward the calls. Various services based on VoIP are available.

An even better practice is the use of “phone drops” instead of direct forwarding. Here the team members call numbers assigned to each one of them, which is answered by an operator that receives the message and then forwards it to the destined recipient.

Application: Notes: Travel security

Travel is an operational nightmare because records of border crossings, hotel bookings and flights contain personal identifiers. This can lead to uncovering ones identity quickly if an opponent becomes aware of the travel details (places and times).

It is therefor paramount to investigate beforehand if a cover can be used, and to conceal travel information as much as possible. One should therefor never give prices travel destination, time and date of travel, or other travel itinerary data to anybody. Furthermore hotels should be booked and paid under cover, and no meetings should be held there – including being dropped off or picked up there. Special care must also be taken to prevent information leakage by having key cards, boarding passes or luggage tags become known to an opponent at all cost. They should be concealed, and destroyed at the earliest moment possible.

When asked about travel dates it may become necessary to give out false information that is a few days off. The same applies to routes taken.

Application: Notes: Travel: Be early, leave late

When traveling to/from meetings one should be early and leave late to conceal travel information to opponents and to be able to do thorough cleanup after and good reconnaissance beforehand (which does not mean to stick around visibly).

It is in general a good idea to establish a large time frame around meetings for above purposes, and to be always punctual.

Application: Notes: Travel to/from meetings

To conceal travel to/from a meeting or operational area, the following method should be employed:

- Have a (large) list of locations that are part of the baseline and that have no other operational purpose then this protocol.
- The home location is defined as Point H. The meeting location as point O.
- **Randomly** pick one of these locations to travel to before traveling to the meeting. Point T.
- Pick another location for traveling from the meeting. Point F.
- Latest at these decoy points all pockets, wallets, bags, vehicles should be cleaned from litter and possible trackers/bugs.
- If a cellphone is carried, it should be dropped off at point T. When traveling back, first travel to

point F, do the cleanup, then travel to point T to pick up the phone. The same applies to other items that need to be carried from point H but should never be present at point T.

If no list of locations matching the baseline exists, as for example when operating away from home, either select a random tourist attraction (or other point of interest with a cover) or a random place on the map.

Application: Notes: Travel: Air travel

Giving up ones luggage anytime before having to cross a security checkpoint, customs or passport control opens up an opportunity for the opponent to frame the target or place trackers.

The operative thus should thoroughly search luggage immediately before checking it in, going through security and directly after claiming the baggage. This should happen in an undisturbed place, like a public toilet.

Application: Notes: Travel: Secure room (hotel or home)

Rooms are a primary target for the opponent for surveillance, collection of forensic evidence, collection of documents or other artifacts, installation of malware, planting of false evidence, and more.

Various tactics need to be adopted.

First, never leave anything in the hotel room if you can carry it. Specifically one should never leave ones computer and documents (except for identity documents in the hotel “safe”). Things not present in the room cannot be manipulated or stolen when attacked by the opponent.

Second, it is necessary to be able to detect entry and searching or manipulation of the room. This requires that innocent entry is prevented – use the do-not-disturb sign and lock the door if possible. Furthermore place and memorize objects in the room in a non-orderly fashion. Do not align objects towards each other – the room should look messy, but fully controlled by you. Do use **tells**, hard to detect objects that are easily disturbed. For example stretch a black thread between the chair and the bed just above the floor. Moving the chair should easily undo the thread. Do not use tells close to doors or windows where an attacker is most likely to look for them and raise attention when one is detected. Another tell is to use a crisp put below a rug, mat or carpet. Walking over it will break it but it looks innocent enough (it has a “cover” of being just a dirty room). Technical tamper evidence can also be employed, but it is hard to conceal and will raise “credibility”. Be aware that alignment of objects is NOT a good method because it is easy to replicate using photographs which is a standard technique these days. For all tells, make them hard to repair if disturbed and make sure you check the tells well.

Third, always close the curtains while you are in the room to hinder remote video surveillance. Also

use music to make audio surveillance harder. Be aware that both methods are not perfect.

Fourth, be aware that many hotel rooms have been spiked with surveillance equipment already. Especially above the desk, facing the bed and sometimes the bathrooms. Be aware to not have private conversations in the hotel room, over the room phone. Do not place your documents on the desk for reading or your computer for working. Instead, move the desk a bit or use a blanket to prevent viewing the keyboard and ideally the display. Best is to avoid the desk completely.

Fifth, whenever entering the room sweep it for placed objects. An opponent might want to place false evidence or surveillance equipment. A previous guest might have hidden drugs or weapons himself and forgot about it. Make sure your room is “clean” and nothing in it can be used to frame you. This is especially important for luggage, clothing and the safe. The sweep must be repeated every time the room has been unoccupied for any time. Also be careful with room service. Do not allow entry to the room when ordering food but accept it at the door. Room service will look around in the room and/or drop something.

Sixth, if possible use a door blocker/alarm while in the room, and lock the door (including the security lock or chain). Cover the door viewer with a small piece of tape – it can be used to look into the room. Use the door viewer before opening the room. If available, use video surveillance while in the room and before opening the door – a tablet/computer will do the job. It helps collecting evidence in your favor and help with detecting attacks.

Seventh, if available and the operational profile demands it, use video surveillance with tamper evident and/or offsite recording. Be aware that use of security technology will raise suspicions and attention by the opponent if he notices.

Application: Notes: Signals, Alarms, Fallbacks

In the context of meetings, hand-overs, deliveries, brushes and dead drops signals should be employed to communicate “all clear” or “danger, abort”. These signals should be arbitrary and unsuspicious so they don't draw opponent attention or can be understood by him.

In case of an abort signal a fallback/emergency plan must be in place. For example the route to a safe house and the time and location of an alternative meeting.

Application: Notes: Caches (physical and digital)

For isolation and recovery purposes caches are an important tactic. Caches are places to store objects that are not directly associated with the operative.

Physical caches can hold cash, cover-related objects, escape identities, tools etc. They must be long-

term viable (not easily found/destroyed by accident), concealed and accessible in should the need arise. Occasionally caches must be checked if they are still in place. Furthermore caches should be tamper evident and should only hold information relating one specific task so that discovery does not lead to broad breaches.

Caches that are used regularly should be located near regular routes. Caches for recovery purposes must be outside of normal routes so they cannot be used as pickup locations for surveillance or attack.

Whenever a cache is created, checked or otherwise accessed anti-surveillance methods must be in place and the surrounding should be observed before making a move towards the cache.

Caches should be accessed infrequently so that they do not become convenient surveillance or collection targets. For operational caches, for example those containing regularly used objects related to covers, frequent rotation should be employed. Whenever tampering with a cache or surveillance of a cache is detected, the contents should be considered toxic and the cache should not be accessed ever again. Contingency protocols concerning the objects/information in the cache must be employed at once (notification, destruction of related artifacts/information, cleanup).

Digital caches for important information should be paid anonymously and for long periods in advance. Access should only happen when necessary and for infrequent verification. Access must use anonymization techniques. All data stored in the digital cache must be encrypted. Access details should be memorized so the cache remains useful even if other storage and computing has been compromised or lost.

In general there is a trade off between complexity of caching operations and need-to-X principles. It is important to not be lazy in this regard. Caches should hold minimal artifacts/objects/information (separation), never hold objects/information relating to multiple operational contexts (compartmentalization), and be unrelated in makeup and location (isolation).

Application: Notes: Temporary caches, lockers

While going into operational areas it is important to leave anything behind that is not absolutely necessary. In some situations this is difficult because the distance between operational area and base is too large. For example, bringing identity documents to meetings is bad practice, but leaving them at the hotel might be too risky.

For this purpose a temporary, one-time caches can be employed. Various options exist. Storing luggage with a different hotel, using lockers at transportation hubs (attention, surveillance!), gyms/swimming pools, shopping centers etc. is one option. These places are often viable to store extra clothing and camouflage as well as access to unobserved areas (toilets, cabins to change) which allows modification of appearance and deep cleanup before and after operation.

Application: Notes: EDC, Bugout bag

A bugout bag containing cash, identity information, emergency contact information, emergency tools, communications equipment, camouflage, medication, clothing, high protein food and unvalidated tickets for local transportation should be created. This allows the operative to quickly withdraw on a moment's notice. Such a move might be necessary whenever a leak/breach/opponent attack has been detected but no damage assessment has been yet performed. The ability to get out of any immediate danger greatly improves stress and results. A bugout back must be easy to access (possibly in an emergency cache) without revealing additional information to the attacker. What has been said about caches in general also applies. Furthermore the bugout bag should be cleaned (searched for manipulation, planted evidence, planted trackers) as early as possible and before making any distinctive moves.

A bugout bag loses its value if the operative is not prepared to immediately use it. This means that all places of operation should be clean at all time and that destruction/cleanup procedures can be enacted quickly and effectively. Escaping while leaving behind critical information/artifacts will only increase the damage, not mitigate it.

In addition the “every day carry” should be planned and assembled to allow for minimal escape and recovery options if the bugout bag becomes inaccessible.

Application: Notes: Payments

Whenever possible use cash for all payments. If credit cards are unavoidable use prepaid anonymous debit cards. When using cash, make sure to have it exchanged after withdrawing it from an ATM and before using it for any operation related payment. Cash from one operational context may never be used in a different operation. The same applies to credit cards, Bitcoin addresses or bank accounts.

Application: Notes: Air gap computers

Certain data storage and processing tasks are too delicate to entrust to networked computers. In this case air-gapped computers are used.

Air-gapped means that there is no network that connects this computer to any other system except for asynchronous, manual data transfer.

These computers should boot only from read-only, immutable media, consist only of the minimal necessary components (processor, ram, media access, display, keyboard), and be stored in a secure and tamper evident manner.

Transferring data to the Air-Gap computer must employ only write-once, read-only media like CDRs or

DVDRs. USB stick, portable hard discs and SD-cards are no option because they have processing abilities themselves and can be written to multiple times. Any media used with the air-gap computer must be immediately destroyed after the data has been transferred.

For transferring data from the Air-Gap computer to any other system must use the same methods. However, transfer from the air-gap computer should be the absolute exception.

All transfer to/from the computer should also happen through encrypted text files. No complex data formats should be used. They must be visually verifiable without needing complex interpretation by any software. Encryption should use per-media keys only that are randomly generated and never reused. Furthermore integrity protection of any transferred data should be employed.

An Air-Gapped computer can be equipped with writable permanent media only if this media can be removed and it is encrypted and integrity protected. When using writable media, no “incoming” media should still be attached to the system. After initial processing and storage of incoming media the system should be rebooted from the read-only boot medium to reduce attack persistence.

Should an air-gapped computer be used in multiple operational contexts, it should be rebooted into a clean state whenever the context is switched. Writable permanent media should always be reserved for a single context. Ideally every context also comes with its own operating system installation and its own hardware, if feasible.

Air-gapped computers should ideally be contained in a complete Faraday cage, be sound-proved and be sealed. They should also be visually verifiable and should carry tamper evident markers.

If possible such a system should always be procured from a randomly selected source that is physically visited for procurement on no or very short notice.

Application: Notes: Dead Drops

Dead drops are caches that are used to transfer information/artifacts from one person to another. They can come in digital and physical forms.

A physical dead drop should qualify as a cache (see above) that can be accessed without raising attention or suspicion. This also means that it must fit into the baseline movements of both parties (sender and recipient).

To signal if a dead drop is filled and ready for pickup, a signal should be created at defined place so the recipient can read it. After the dead drop has been emptied an optional “empty” signal can be employed. Accessing the signals and accessing the dead drop should happen separately and not during the same movement. Always return to Point H between those actions.

Physical dead drops can be reused, but should be given up and exchanged frequently if possible to limit their effect on the operational profile. All access to a dead drop is a risk, they must be employed with

caution.

In certain cases surveillance of the dead drop and a danger signal can be employed. However, using surveillance increases the operational profile and can increase the risk of detection.

Digital dead drops must only be accessed through anonymous communication means and may only contain encrypted information. Digital dead drops may never be reused. They are always throw-away.

A special case of physical-digital dead drops exists. These can be public wifi networks, or custom hidden wireless networks that are temporarily set up for data exchange.

Physical-digital dead drops can be an extremely effective means for cover communication if they are:

1. Self destructing and use encrypted ephemeral storage.
2. Short range.
3. Have cover (such as mimicking a corporate network) or public hotspot.
4. Use encrypted communication.
5. Wifi security (see above) is employed.
6. Activated only some time after they are deployed.

Using drop&forget devices (throw away, automatic upload/download devices) that use long (multi-hour) random delays before activating further increases security for the involved parties. Their downside is complexity and cost.

Application: Notes: Brushes

Brushes, or brush passes, are quick person-to-person exchanges of information/artifacts. They are quicker and cheaper to set up than dead drops but harder to execute and easier to attack by an opponent.

To set up a brush the parties have to agree on place, time, signals and makeup of the object(s) to be exchanged.

Locations of brush passes may never be used again, and they must be plausible within the movement baseline of both parties. The locations should provide good anti-surveillance qualities.

Timing must be precise and strictly adhered to. This invites operatives to “linger” before the brush, which must be prevented at all cost. Dynamic timing should be employed (one party waiting without raising attention, then picking up the second party after exchange of signals).

Signals must include “danger” and “ready” as well as mutual recognition.

The exchange must be quick and not change the appearance of any party. This may require both parties to appear carrying equal containers. Be aware that even the weight and flexibility of the containers

(including contents) should be the same.

At least one of the parties employed in the brush should never be used for a brush with the same party again to prevent recognition by the attacker.

In general, brush passes should not be employed unless absolutely necessary.

Application: Notes: Rally points

In case of recovery any team/group should have a list of predefined rally points to regroup. Ideally these points differ for every member so that compromise has minimal effect. Rally points should be easy to access but outside of operational areas and the baseline of any operative. They should provide for multiple exits and basic anti-surveillance. Accessing the rally point frequently should raise no suspicion. Any operative appearing at a rally point should be vetted and checked again.

A common method for rally points is to define a cafe, restaurant or square, one or more weekdays and times. Furthermore signals for danger and “all clear” must be defined. If possible the operatives should be able to use a secondary signal at another point to notify others that they are ready to meet. This signal must be easy to observe. All access to rally points and their signals should only happen with strong anti-surveillance to ensure that opponent action is stopped short.

The presence of both parties within the same area must be minimized, parties should exit the area in opposite directions.

Application: Notes: Face to face meetings

Occasionally parties have to meet face to face. Meetings should take place at mutually determined places that fit the baseline of both sides. Signals for “ready” and “danger” should be employed. Before meeting one party should “pick up” and do some basic counter-surveillance on the other party, ideally with the roles being reversed.

In general meetings should not occur within proximity of CCTV installations, never in private homes connected to the parties, never in cars, and never in repeat places. Ideally the meeting should be possible without the opponent noticing that a meeting takes place. Basic camouflage should be employed if possible to reduce the effectiveness of image surveillance. If possible the meeting place should be hard to overlook, it should be as deserted as possible, and ideally also provide some background noise. People approaching the location or lingering there should be easy to spot. Beware of invisibles: Bums, cleaners, street merchants etc. Also be aware of hidden cameras (like wildlife cameras).

An ideal place are forest parks with recreational activity but many quiet spots. Walking while talking

reduces the ability to detect surveillance in such environments. If possible counter-surveillance should be used.

Meetings should be used rarely, and should be as short as possible. Usually they are both unnecessary and come with high risk.

Instead, meetings should be intersections of both party's baseline. Like attending the same regular events. This provides good cover not just for being there at the same time but also for interacting with each other.

End note, Twelve commandments:

This text is all but exhaustive. Much more could be said. There's no end of it. However, good OpSec is not about having a lot of knowledge. It is about discipline, common sense and creative use of imaginative powers to come up with new methods – and varying them frequently.

1. Never let anybody know your capabilities, your assets, your skills, your relationships.*
2. Never let anybody know your plans.*
3. Don't trust anybody.
4. You're always under surveillance.
5. Do not cache incriminating objects where you live or work.
6. Keep operational activities and personal live strictly separated.
7. Always clean up everything. Don't carry what you don't really need and know.
8. Never mix activities, operations.
9. Do not come into contact with the opponent. Do not talk with the opponent. Do not greet the opponent.
10. Maintain your activities within your own skills, and the skills of your crew and contacts.
11. Shut up.
12. There is no break while you breathe.

** exception apply where operational necessity exists.*