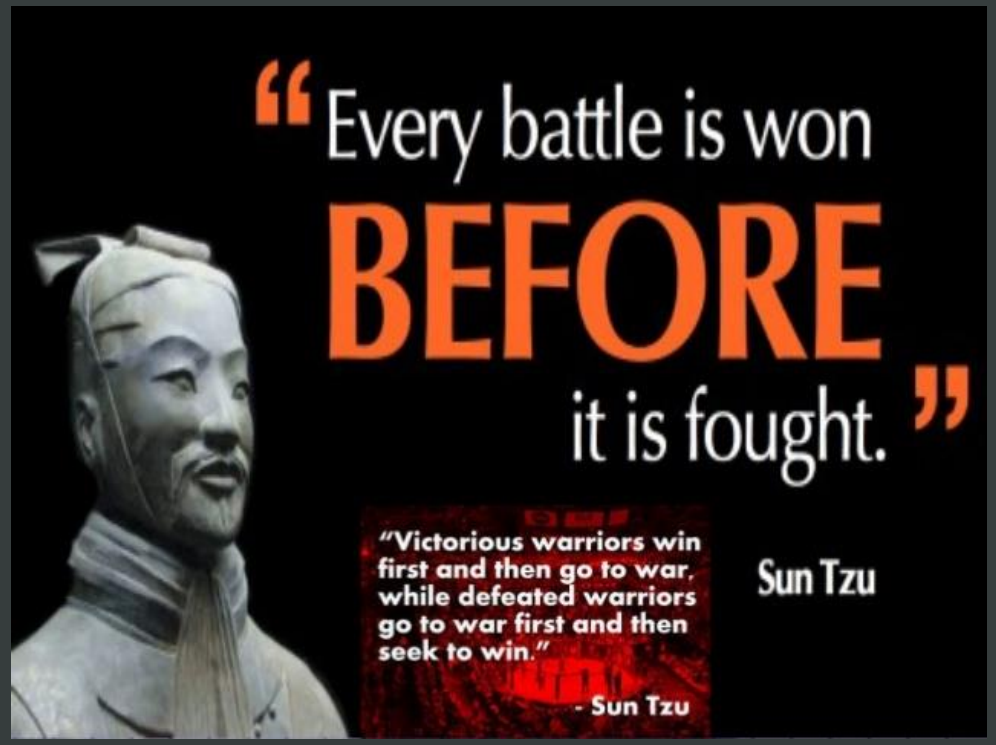
OSINT

BY – APURV SINGH GAUTAM



SUN TZU -- Art of War

- If you know your opponent weaknesses and How to exploit them you will never loose.

Intelligence Gathering

- Intelligence gathering is a process of collecting intelligence(data) from various sources.

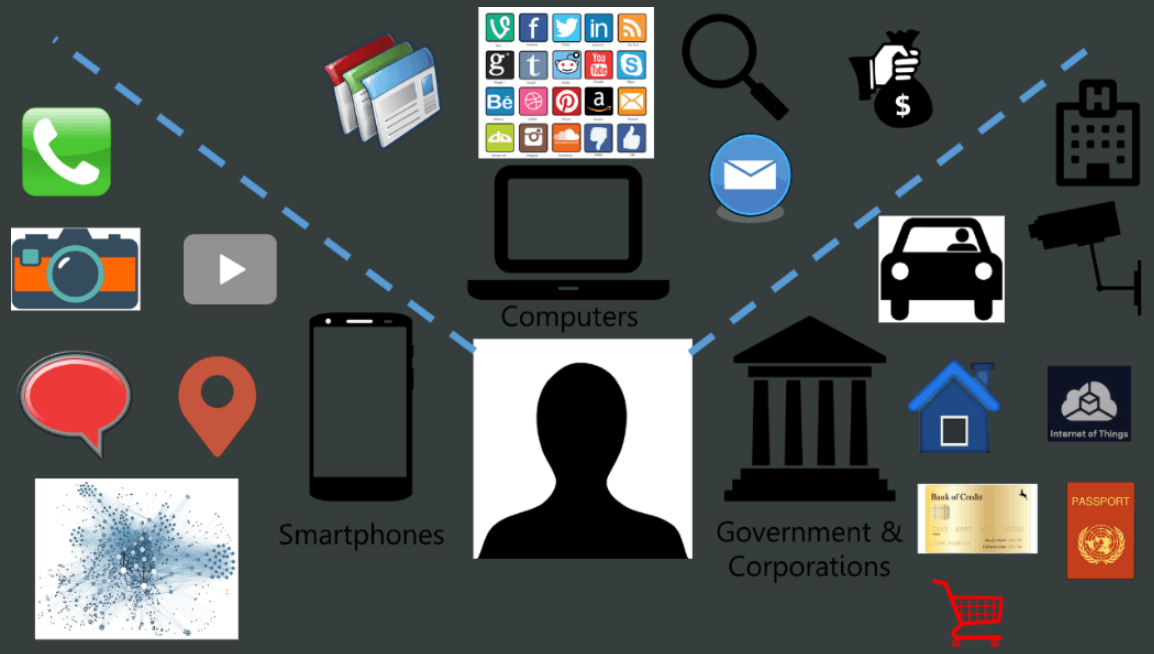
↓

Open or closed

Intelligence Gathering Disciplines

- HUMINT → Intel gathered from Humans
- GEOINT → Intel gathered from images, geo location and human activity.
- SIGINT → Intel gathered from signals, communication
- TECHINT → Intel gathered about weapons, defense and military affairs.
- FININT → Intel gathered from documents, organizational data and financial affairs.
- OSINT

OSINT ?



What is OSINT?

- Information available publicly from public sources.
- Sources might be -
  - Media
  - Internet
  - Social meetings

What kind of data we can gather?

Main OSINT Search Area

- Email
- Social Accounts
- Real Time Monitoring
- Websites
- IP Addresses
- OSINT for Blue Team and Red Team

OSINT Arsenal

- Search Engines
- People Search Engines
- Social Networks
- Video Sharing Platforms
- Various public API’s
- Tools

Search Engines

- Google
- Bing
- Yandex

TOR Search Engines

- *www.torchtorsearch.com*
- *https://ahmia.fi*
- *https://thehiddenwiki.org/*
- *http://onion.link/*
- *https://tor2web.org/*

Twitter Intel Gathering

- https://moz.com
- http://ctrlq.org/first/
- Google Dork is not a bad option ☺
- Geosocialfootprint.com
- Tweetpaths.com
- App.echosec.net
- Onemilliontweetmap.com
- https://www.allmytweets.net

Social Network Traffic Analysis

- Social-searcher.com
- Icerocket.com
- Socialmention.com
- Delicious.com
- stumbleupon.com
- Keyhole.co

Online Maps | GEOINT

- Flashearth.com
- Here.com
- Google.com/maps

People Search Engines

- Thatsthem.com
- Pipl.com
- Zabasearch.com (For US)
- Intelius.com
- Radaris.com
- Spokeo.com
- Yasni.com
- Advancedbackgroundchecks.com

Domain and IP Address

- Viewdns.info/whois
- Whoisology.com
- Domainhistory.net
- Whoishostingthis.com
- Whoismind.com
- Spyonweb.com
- Sameid.net
- Pub-db.com
- Domaincrawler.com
- Nerdydata.com
- Semrush.com

CT Logs

- crt.sh
- censys.io
- developer.facebook.com

GitHub

- GitHub Commits (Juicy Info)
- GitHub Issues
- GitHub Dorks - https://github.com/techgaun/github-dorks

Thank You