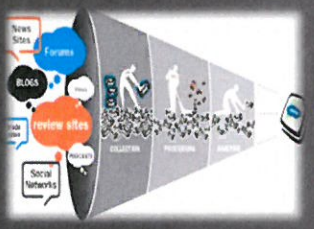
TLP Orange

13/10/2017

ASIS BeNeLux Fall Meeting - Mechelen



Intelligence-Led Security

Defensive HUMINT, OSINT / SOCMINT and GOVINT in support of your security program

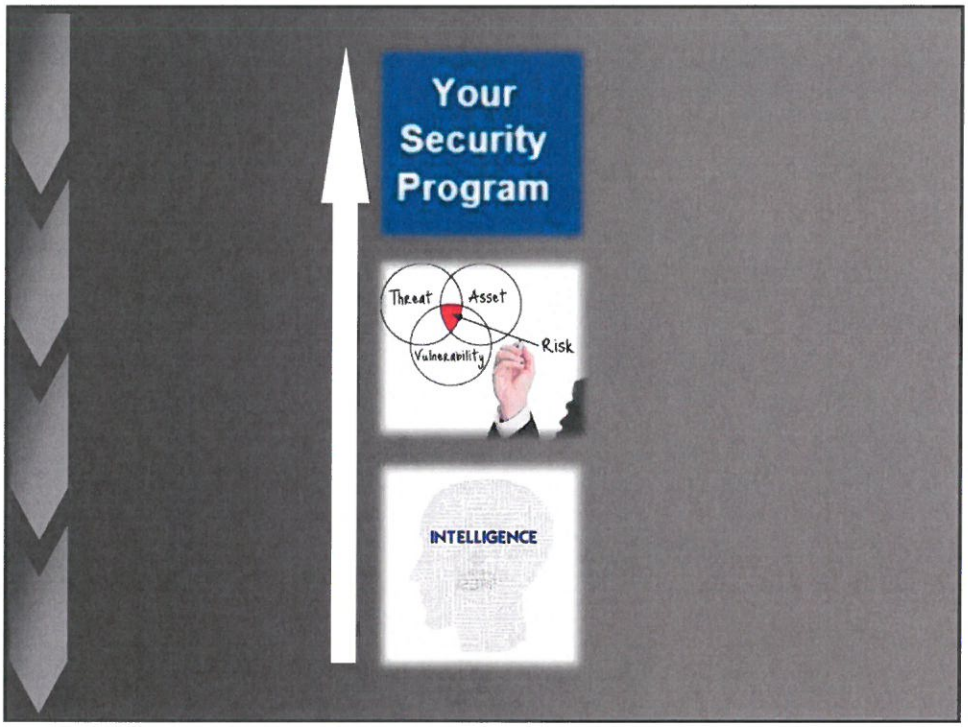
Stephan Van Hauwe

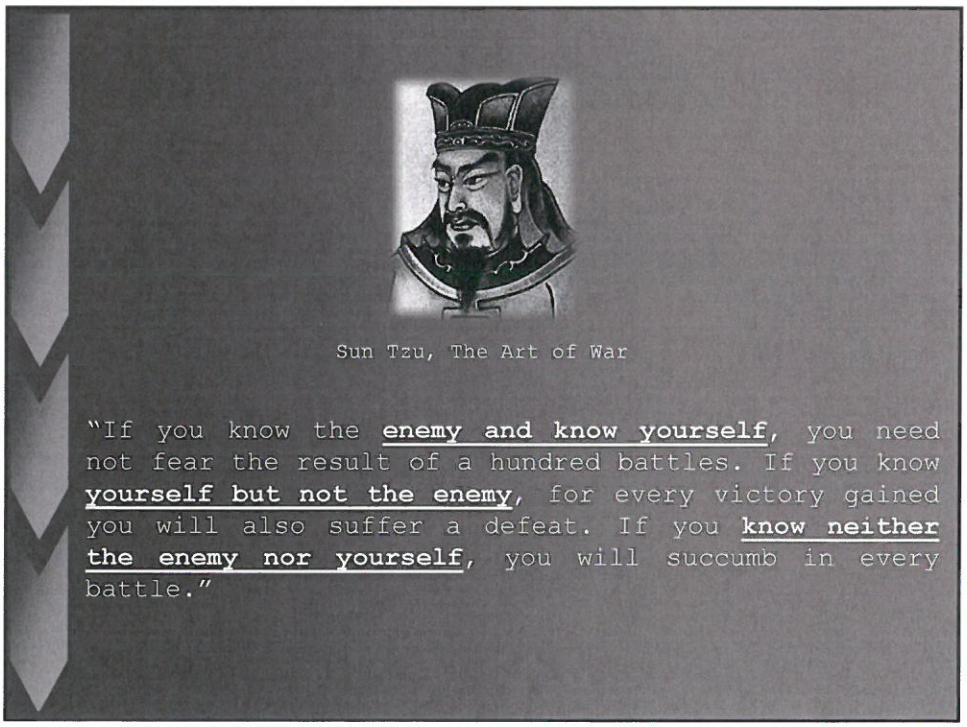
Managing Consultant

OpSeC bvba

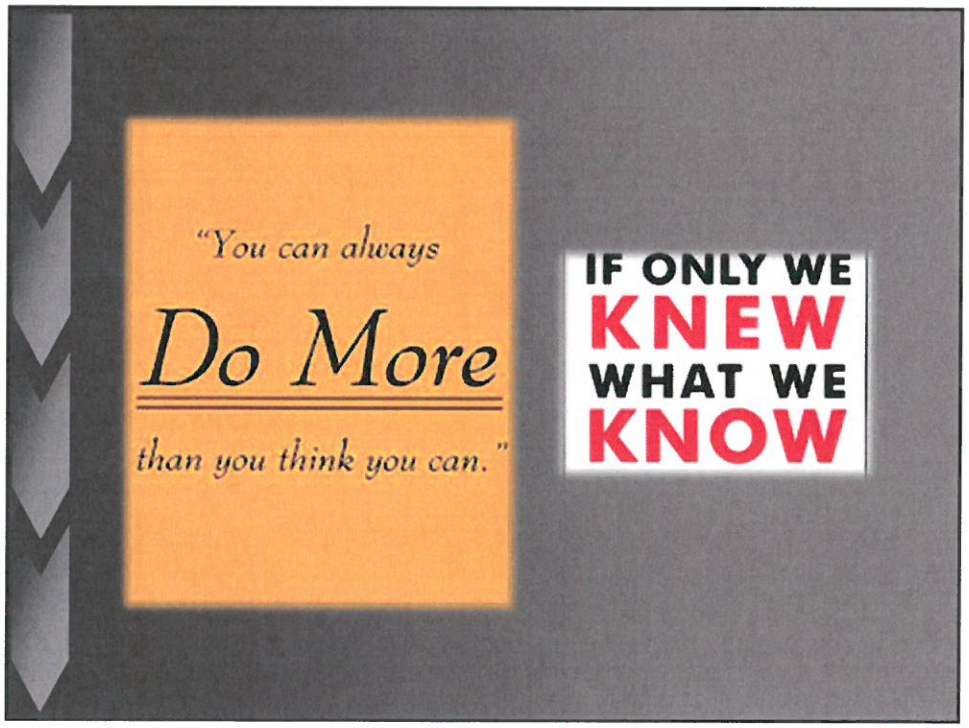
© 2017 OpSeC bvba

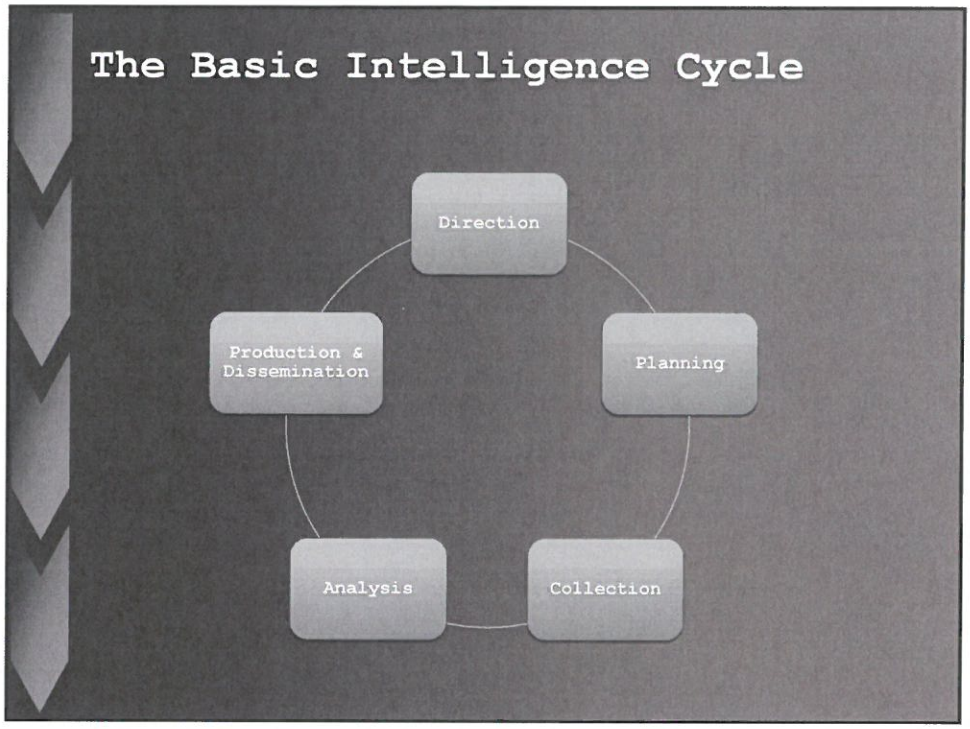
1. Who needs intelligence to support their overall threat/risk analysis and security program?
2. Who has a proactive and structural intelligence program?


Your Security Program
Threat
Asset
Vulnerability
Risk
INTELLIGENCE


Sun Tzu, The Art of War
"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."


I don't know
THAT'S TOO EXPENSIVE
It's the Government's Fault


"You can always
Do More
than you think you can."
IF ONLY WE KNEW WHAT WE KNOW



Intel sources for private companies and organisations

INTEL SOURCE

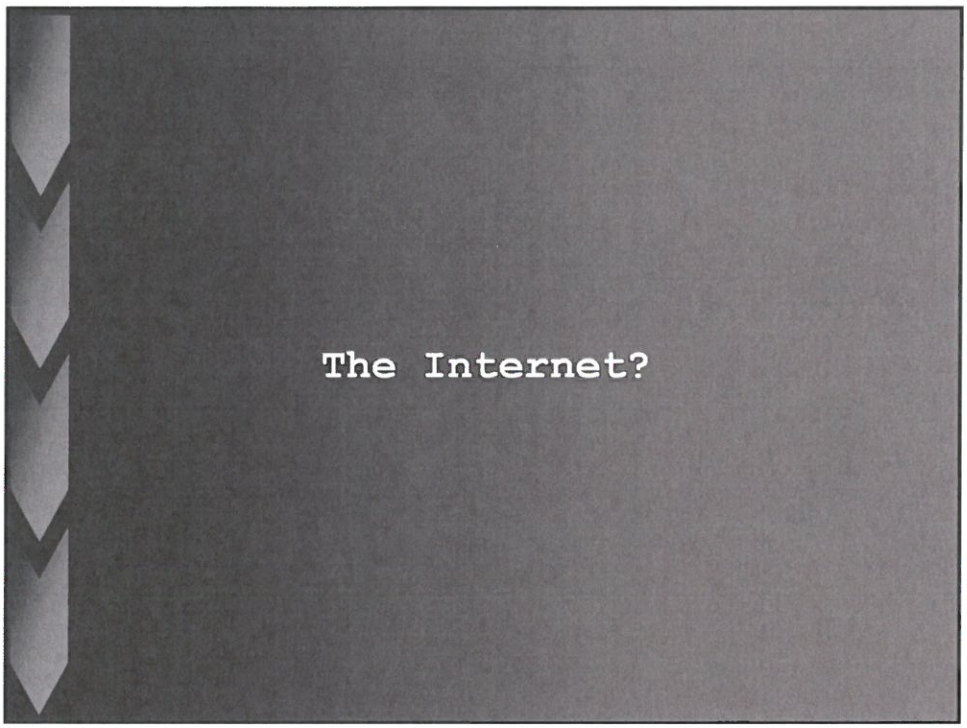
1. HUMINT → ~55%
   1. See - say
   2. Capture - analyse - register
2. OSINT & SOCMINT → ~25%
   1. Structural
   2. Puntual
3. SIGINT (ICT/CCTV/ACS/IDS) → 15%
4. GOVINT→ ~5%
   1. National / International
   2. Direct / Indirect

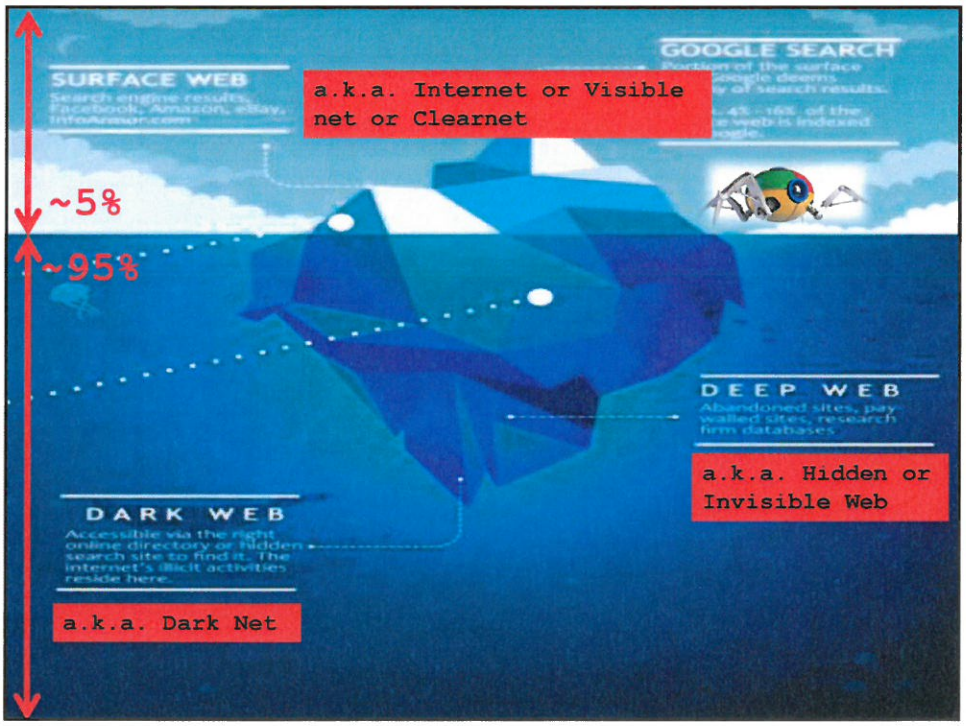
HUMINT

HUMINT network

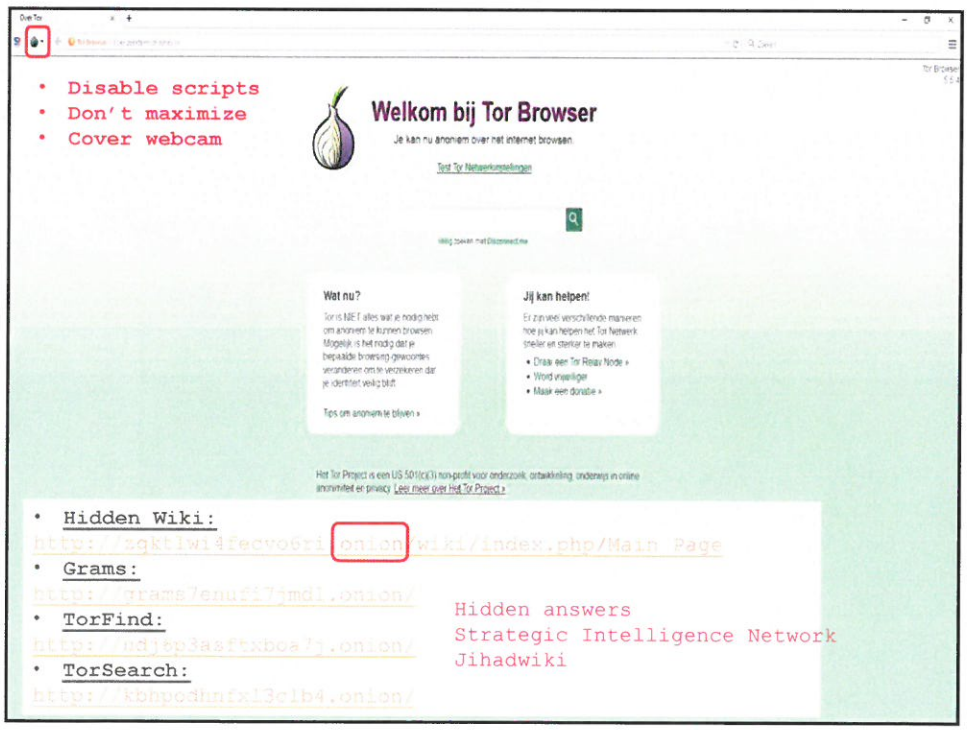
- Population
- Dominant coalition
- Security

- Threat based
  - Indicator driven
    - See-Say
- Unlock a wealth of pertinent, durable and actionable intell
  - See "Strategic and Tactical **Security Awareness**" Network
- Dominant coalition
  - Internal
    - Professional
      - Guard reporting systems
    - Non-professional
      - Staff
  - External (Contractors, Visitors)
- Communication!!!
  - 360°
  - Registration - Analysis - Feedback
- TLP
- Time and energy consuming = high ROI


The Internet?


SURFACE WEB
a.k.a. Internet or Visible net or Clearnet
GOOGLE SEARCH
~5%
~95%
DEEP WEB
a.k.a. Hidden or Invisible Web
DARK WEB
a.k.a. Dark Net

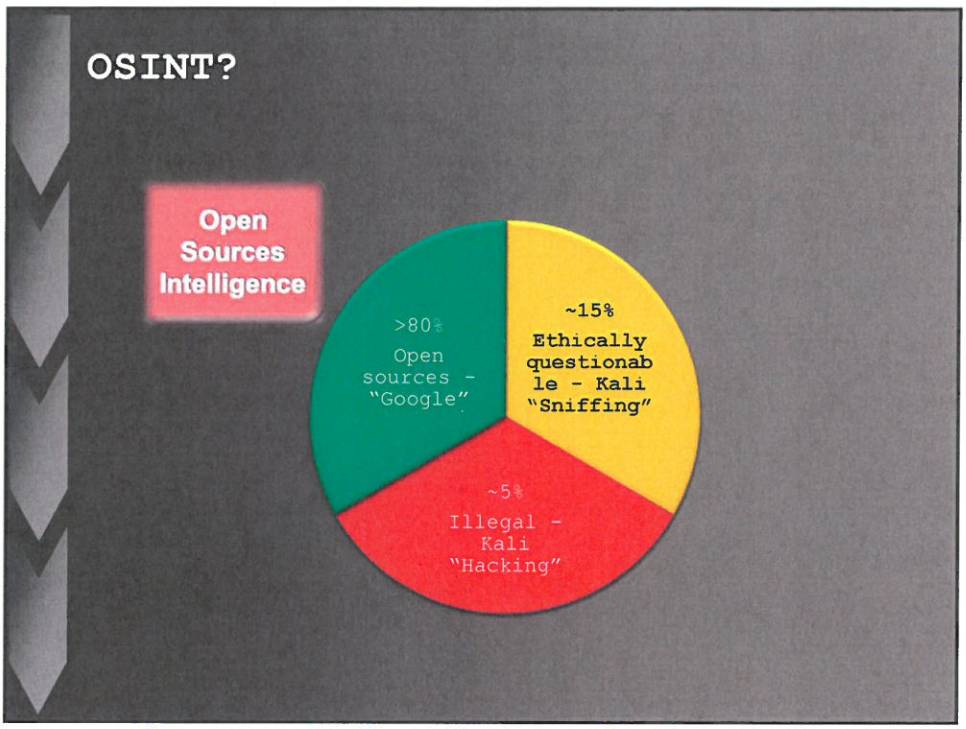

LEGAL
DeepWeb
ILLEGAL
DarkWeb

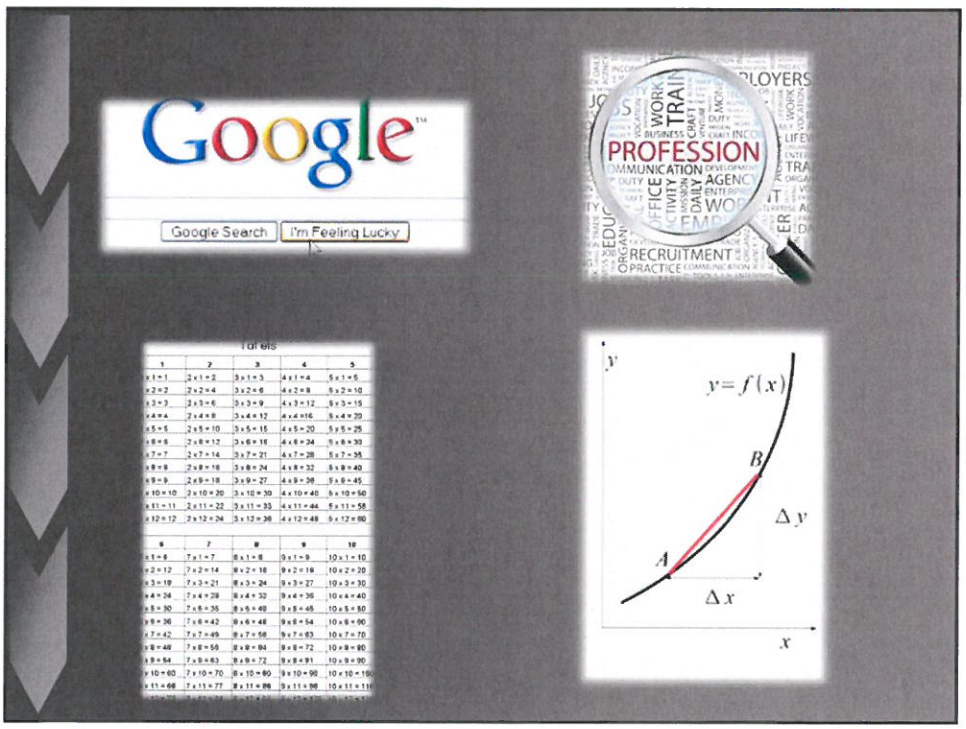

• Disable scripts
• Don't maximize
• Cover webcam
Welkom bij Tor Browser
Je kan nu anoniem over het internet browsen.
Test Tor Netwerkinstellingen
Wat nu?
Jij kan helpen!
• Hidden Wiki:
http://2gkt1wi4fecvo6ri.onion/wiki/index.php/Main_Page
• Grams:
http://grams7enufi7jmdl.onion/
• TorFind:
http://ndjbp3asftxboa7j.onion/
• TorSearch:
http://kbnpo4hnfxl3clb4.onion/
Hidden answers
Strategic Intelligence Network
Jihadwiki

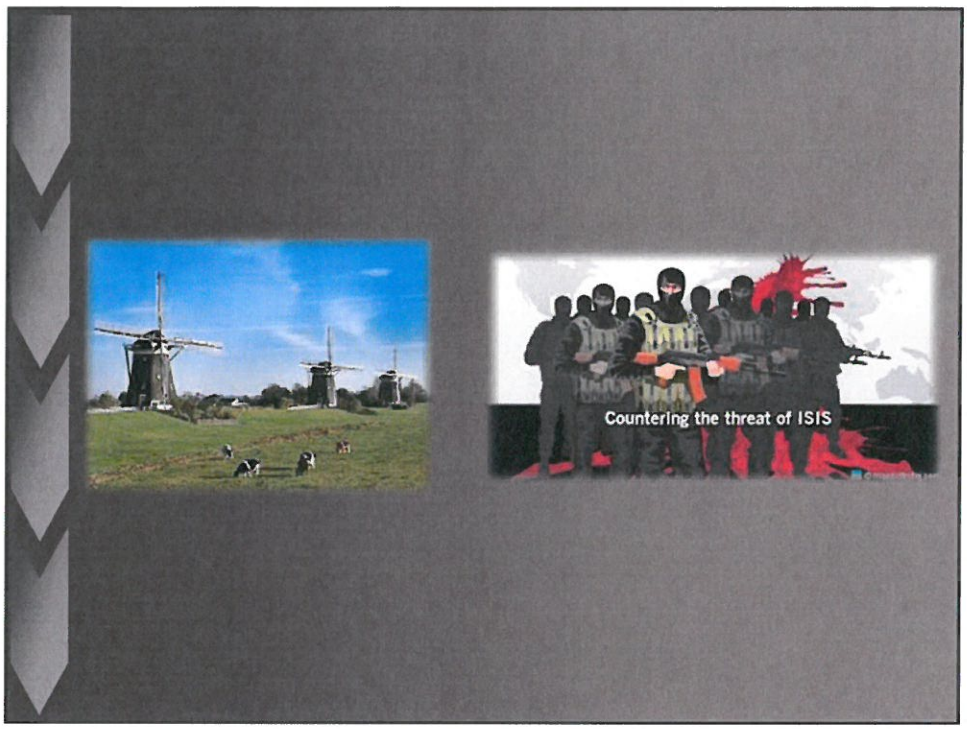
Value of data found on Dark Web

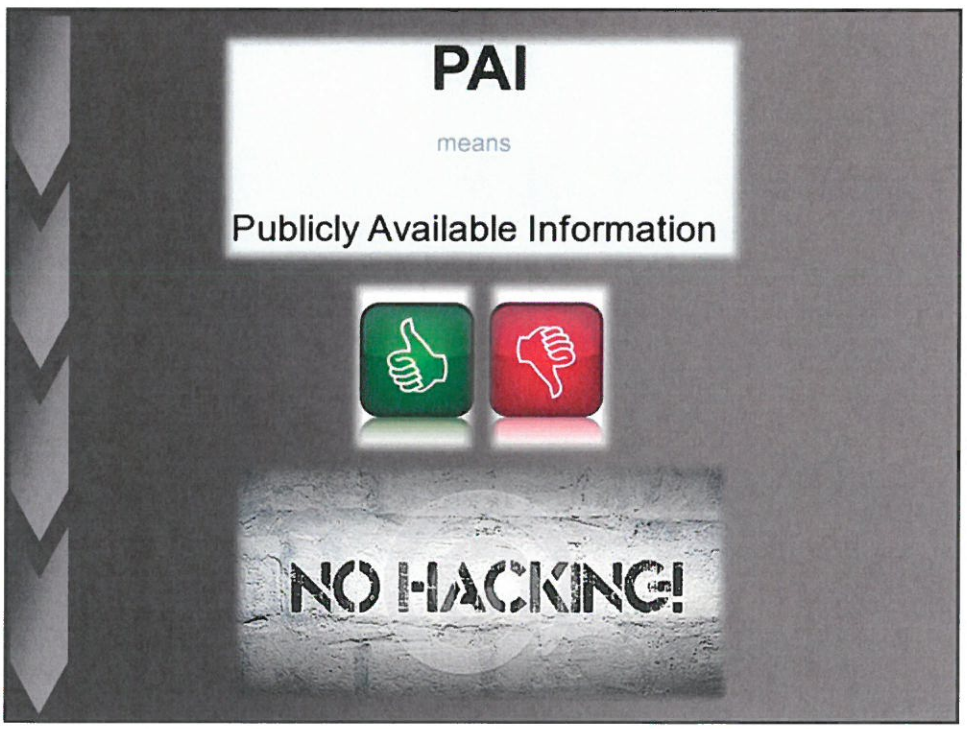
- Understand hacking tools and services
- Detect leaked intellectual property
- Prepare against planned attacks
- Identify and resolve breaches
- Remediate and analyze stolen credentials
  - Consumers
  - Business
- Minimize exposure to third party breaches

OSINT

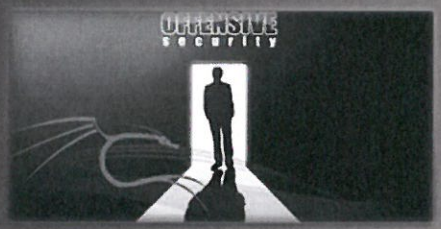

OSINT?
Open Sources Intelligence
>80%
Open sources - "Google"
~15%
Ethically questionable - Kali "Sniffing"
~5%
Illegal - Kali "Hacking"


Google
Google Search
I'm Feeling Lucky
PROFESSION
RECRUITMENT
y
y = f(x)
B
A
Δy
Δx
x


Countering the threat of ISIS


PAI
means
Publicly Available Information
NO HACKING!

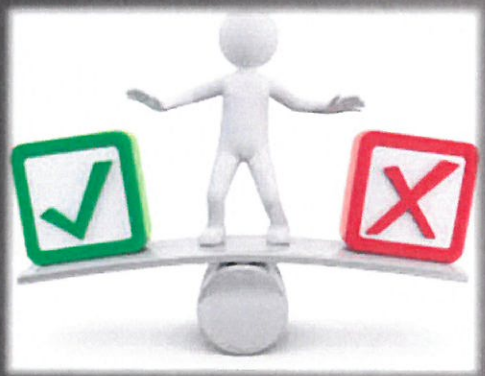
"Ethical" Hacking …

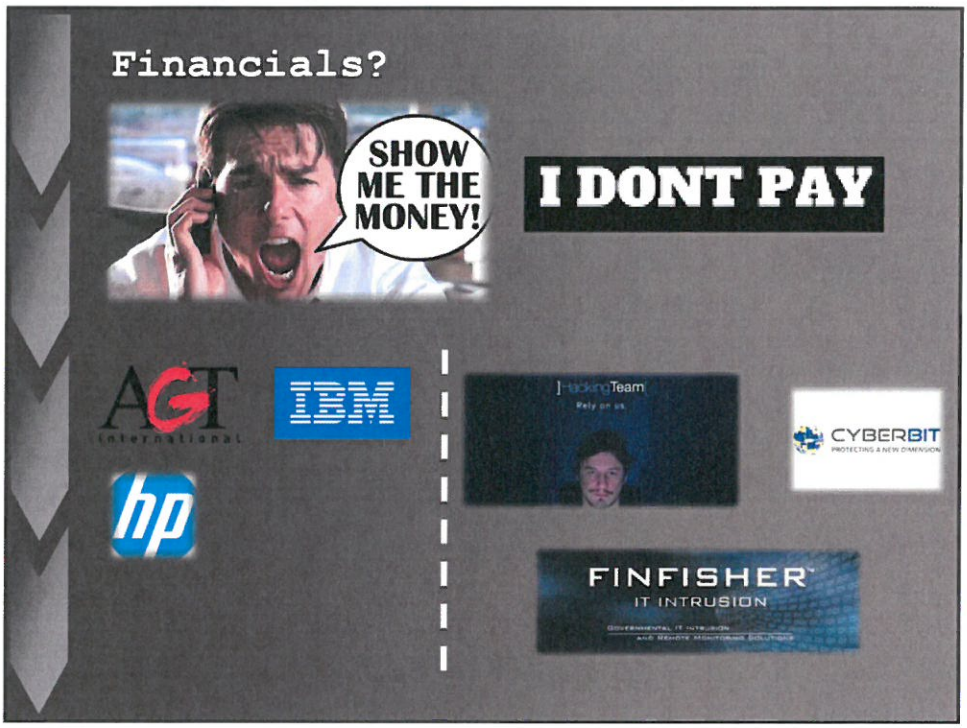


https://www.kali.org/

https://www.youtube.com/watch?v=7nF2BAfWUEg

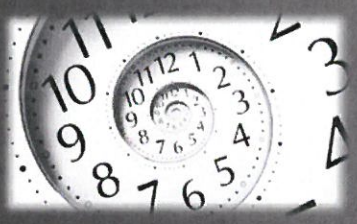
Quid hacked/leaked information online?

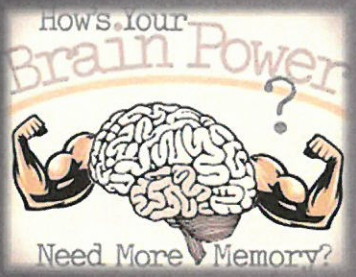



Financials?
SHOW ME THE MONEY!
I DONT PAY
AGT International
IBM
hp
HackingTeam
CYBERBIT
FINFISHER
IT INTRUSION


Attention
BULLSHIT
ONE
STOP
SHOP

OSINT & SOCMINT =





Defensive OSINT & SOCMINT

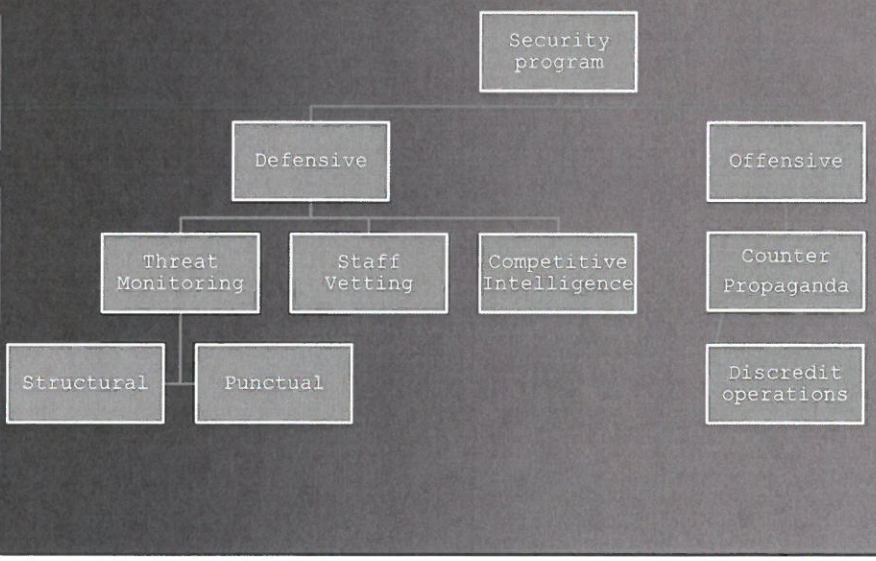
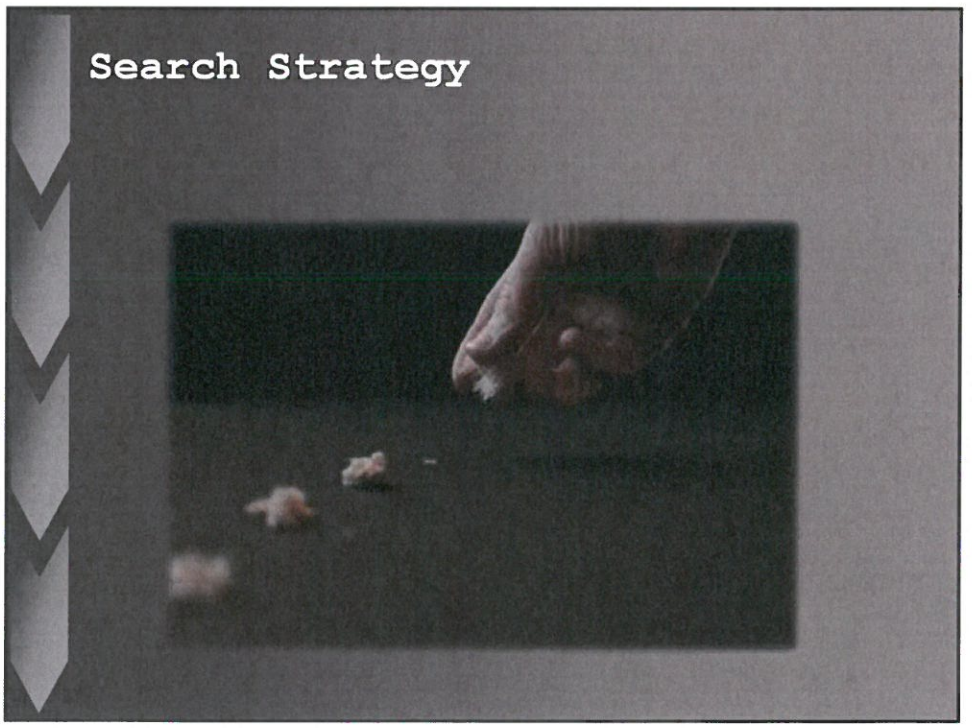
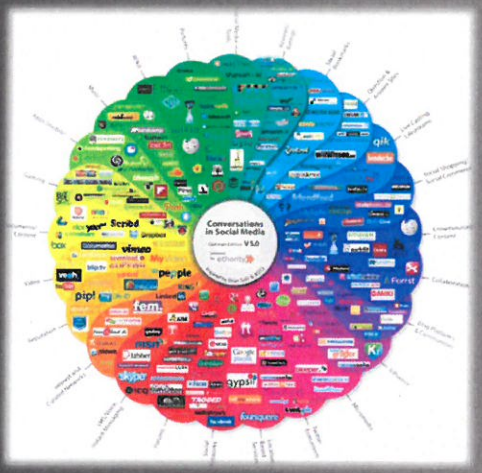


Figure 1. The Fake News Triangle

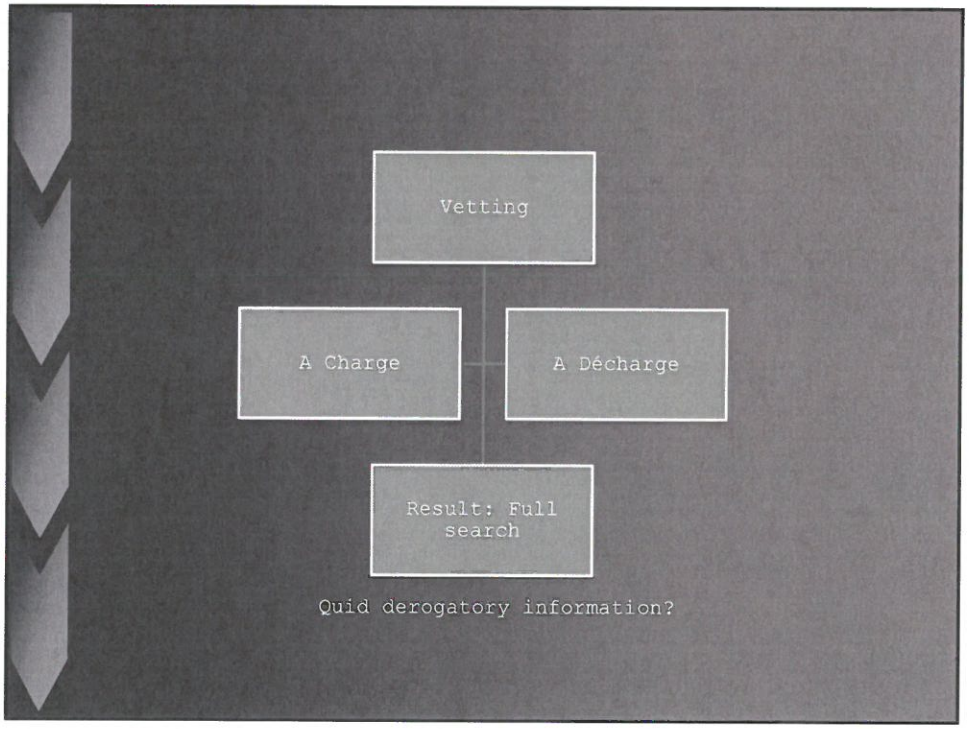


SOCMINT

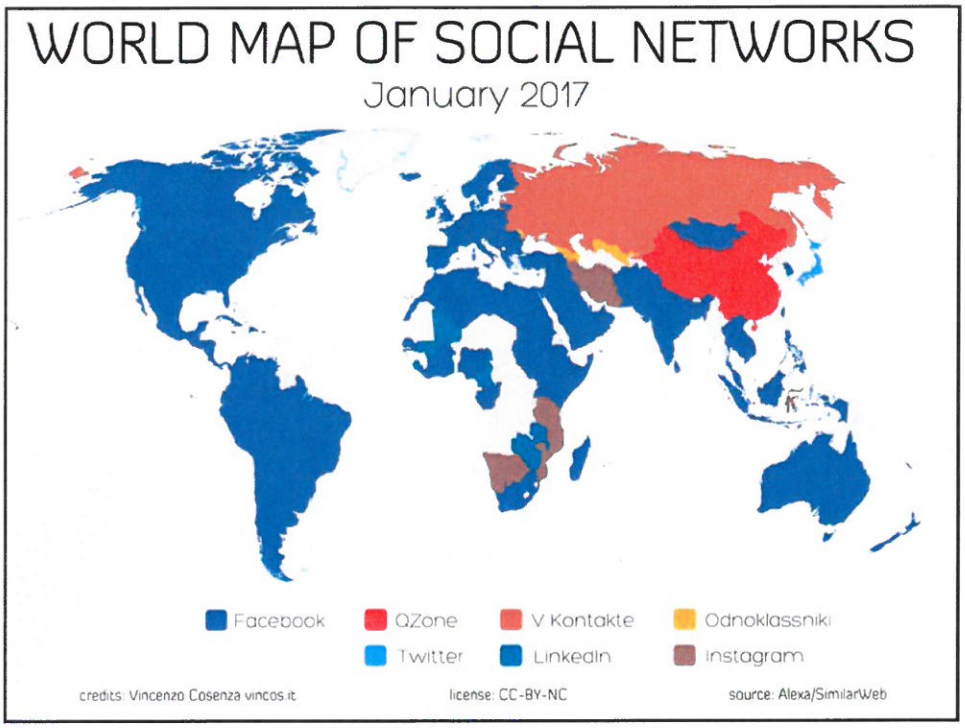
Social Media

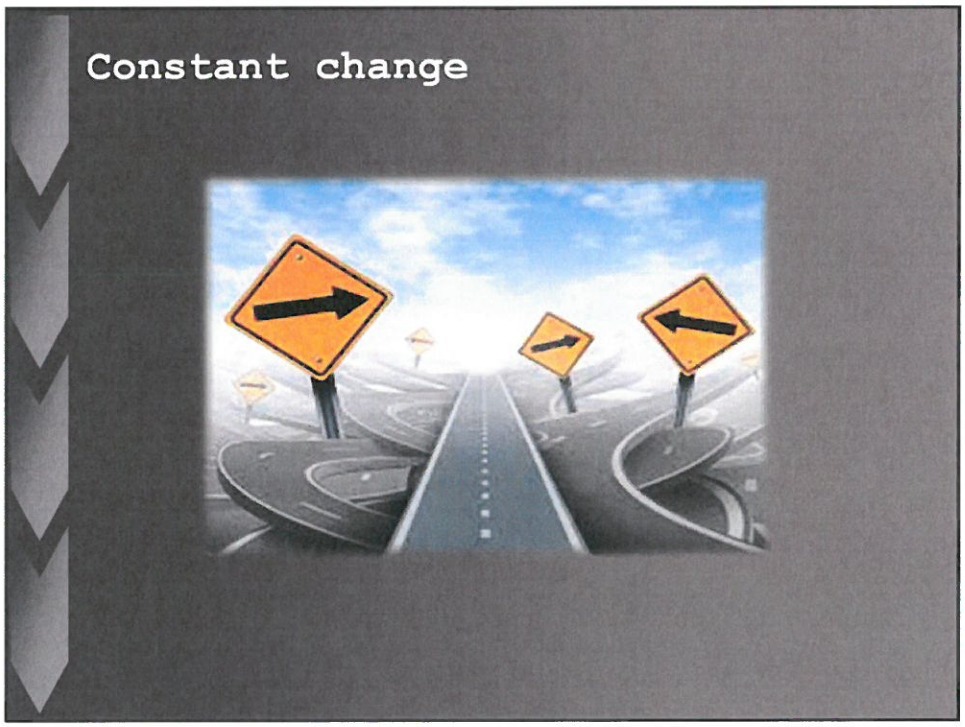


Ensure - alternative - user accounts on principle social media tools



Quid derogatory information?


WORLD MAP OF SOCIAL NETWORKS
January 2017
Facebook
QZone
V Kontakte
Odnoklassniki
Twitter
LinkedIn
Instagram
credits: Vincenzo Cosenza vincos.it
license: CC-BY-NC
source: Alexa/SimilarWeb


Constant change

RTFM

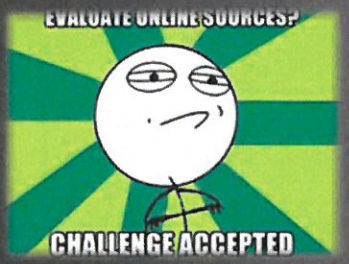
Constant changes

YouTube

Evaluation

Source and Content Evaluation

Reliability, credibility and relevance!



Time consuming!

1. Website
    1. URL
    2. Domain
2. Publisher
3. Author
4. Affiliation
5. Sources
    1. 1st, 2nd, 3rd?
    2. Government
    3. Public
    4. Third party reporting
6. Content
    1. Pictures
    2. Objective
    3. Facts
    4. Opinions
    5. Date - Timings

OSINT Ratings

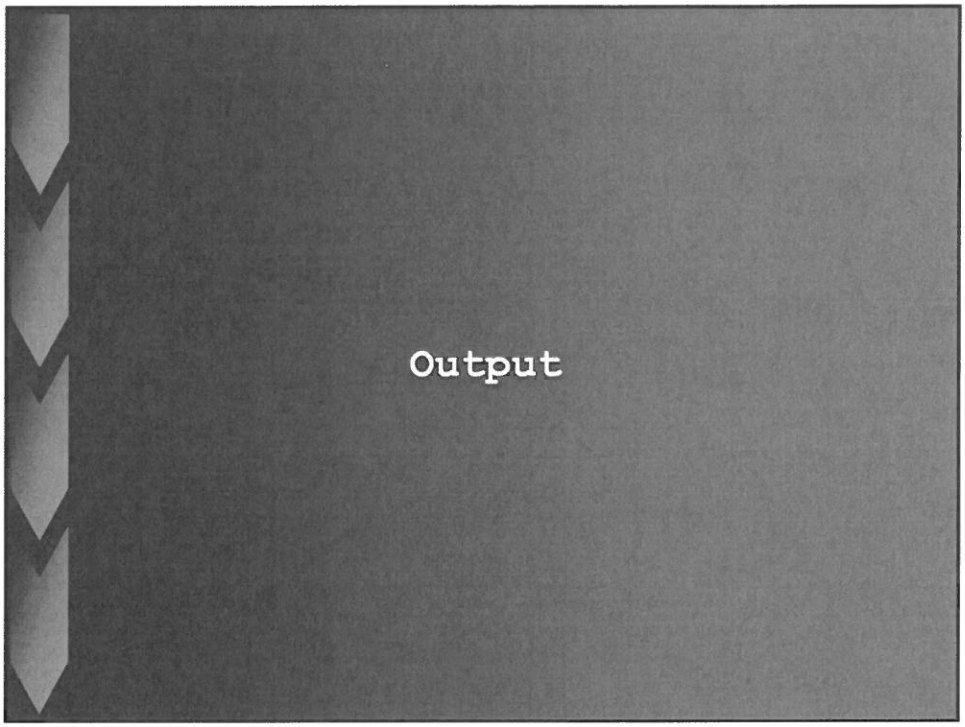
Table 2-1. Open-source reliability ratings

A	*Reliable*	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	*Usually reliable*	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	*Fairly reliable*	**Doubt** of authenticity, trustworthiness, or competency, but has provided valid information in the past.
D	*Not usually reliable*	**Significant doubt** about authenticity, trustworthiness, or competency, but has provided valid information in the past.
E	*Unreliable*	**Lacking** authenticity, trustworthiness, and competency; history of invalid information.
F	*Cannot be judged*	**No basis** exists for evaluating the reliability of the source.

Open Source Information
Reliability and Credibility Ratings
(Source: US Army ATP 2-22.9)

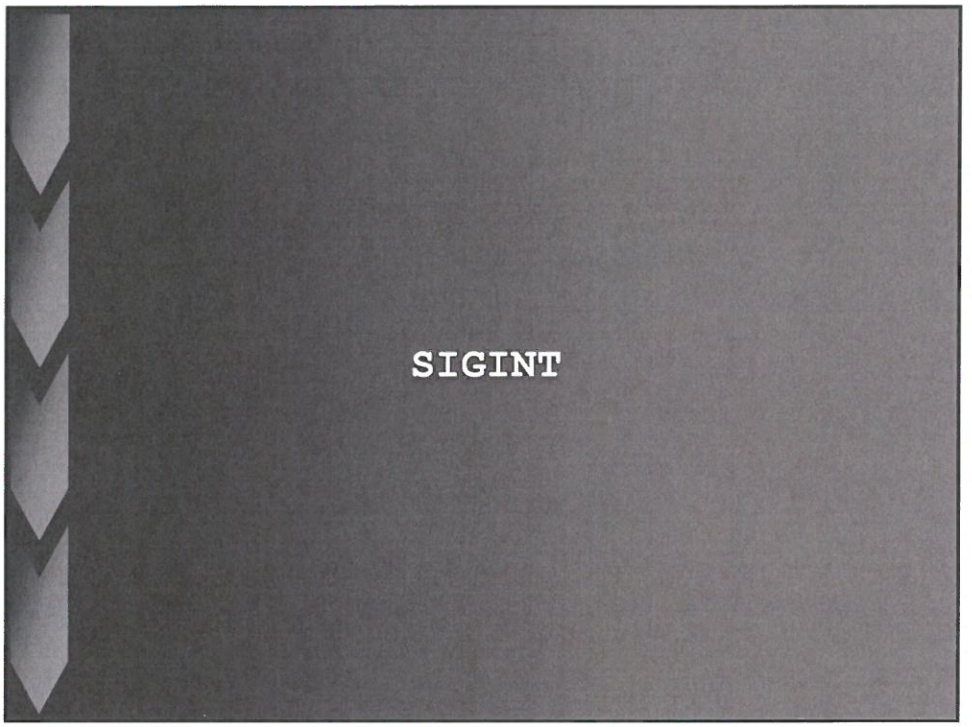
Table 2-2. Open-source content credibility ratings

1	*Confirmed*	**Confirmed** by other independent sources; logical in itself; consistent with other information on the subject.
2	*Probably true*	**Not confirmed**; logical in itself; consistent with other information on the subject.
3	*Possibly true*	**Not confirmed**; reasonably logical in itself; agrees with some other information on the subject.
4	*Doubtfully true*	**Not confirmed**; possible but not logical; no other information on the subject.
5	*Improbable*	**Not confirmed**; not logical in itself; contradicted by other information on the subject.
6	*Misinformation*	**Unintentionally false**; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources.
7	*Deception*	**Deliberately false**; contradicted by other information on the subject; confirmed by other independent sources.
8	*Cannot be judged*	**No basis** exists for evaluating the validity of the information.



Disseminating Intelligence

Who is it for?	What is it for?	How do we present it?
• The final product that an analyst creates needs to be tailored to the requirements of the audience • Remember that the report is for a specific customer who requested it	• Intelligence products must answer the question at hand • Be aware of how the intelligence report may be used to support or challenge policy positions	• Intelligence, if it is not communicated, is useless. • Intelligence products should provide objective assessments, and balanced judgments based on the available facts



Optimizing available systems

SIGINT

- Get more preventative SI's out of your:
  - ICT
  - CCTV
  - ACS
  - IDS

GOVINT

GOVINT network

- Build your trusted network
  - Give - take principle
- The law
  - Official
  - Unofficial
- Levels
  - BE/NL
    - Local
    - Regional
    - External services
  - EU
  - Neighboring countries
- Discretion!

Conclusion

Intelligence-Led Security

FOCUS SECURITY

rosi

There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.

(Donald Rumsfeld)

TLP Orange

Contact Information

- OpSeC bvba
  - Stephan Van Hauwe - Managing Consultant
    - Vergunning FOD Binnenlandse Zaken:54.20.10
    - Ondernemingsnummer: 0502.519.188
- GSM:
  - +32 (0) 477 78 08 58
- Email:
  - svh@opsecbvba.be
- WWW:
  - www.opsecbvba.be

© 2017 OpSeC bvba