i-intelligence

Information as a Weapon

Chris Pallaris | 18 February 2016 I Hackcon | Oslo, Norway

Preliminaries

Information as a Weapon

- Preliminaries
  - Who I am, what I do
  - What we'll cover and how
    - Target scoping using open source tools
    - Data collection for monitoring and vulnerability analysis
    - Organising for effect
  - Legal, ethical and privacy considerations
  - I am here to sell you on the idea of rigour

Information as a Weapon

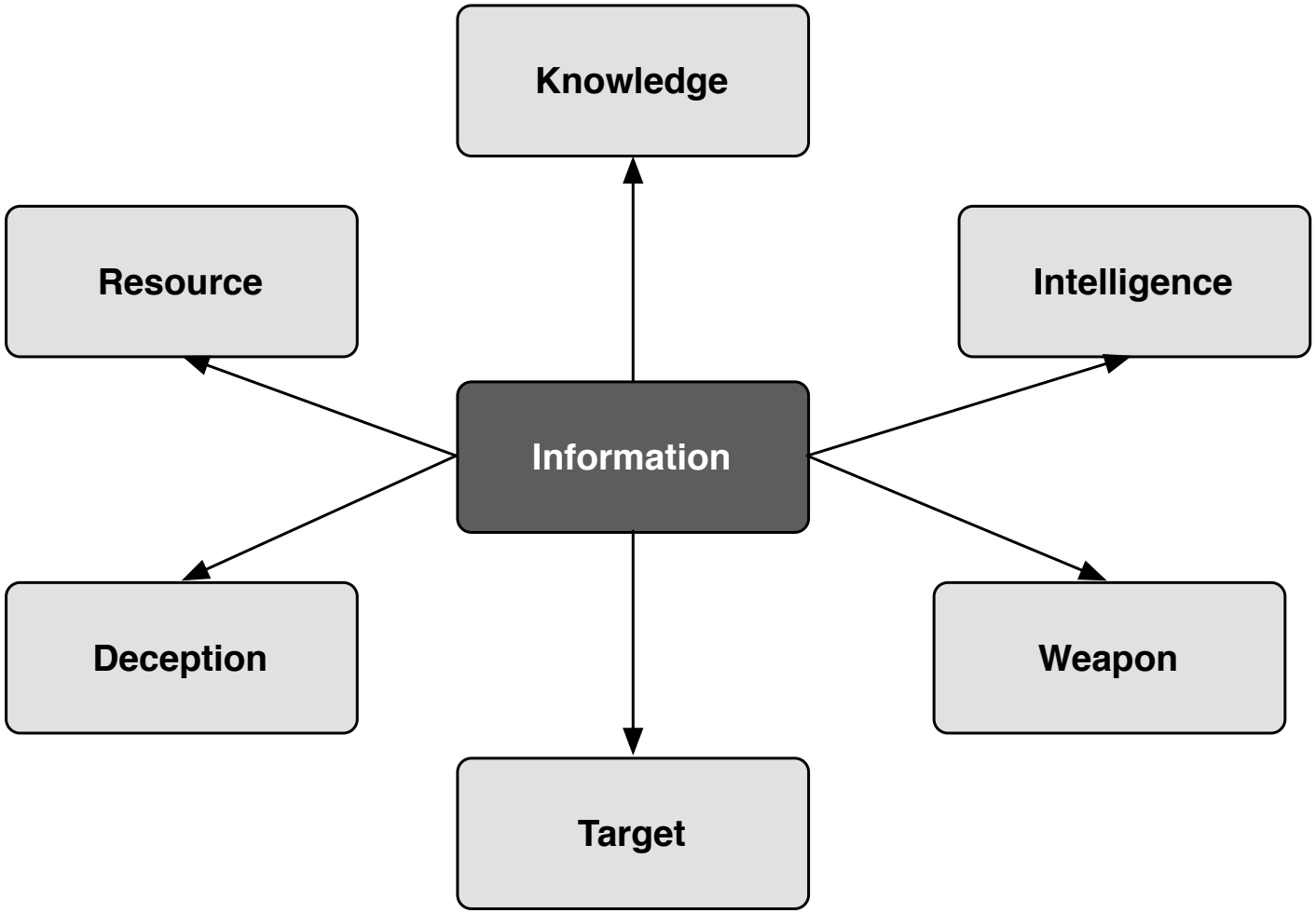
- Conclusions
  - Information has and always will be an offensive weapon. It's potential is best appreciated by those with the requisite ability, opportunity, intent
  - Low level Information Warfare requires structure, rigour, process, diligence, patience and guile. In other words, brains not bits
  - The tools to conduct such activities are freely available and can be used to identify the threats and vulnerabilities to your organisation
  - No single *tool* is sufficient; you need a *toolkit*
  - Countermeasures exist but they require the same levels of rigour and effort, as well as the management of residual risk

Context

Information as a Weapon

- Information
  - Has always been a weapon of war; information technology has not
  - Its abundance enables all forms of offensive and defensive activity
  - Levels the playing field it enables asymmetry and an efficiency of action
  - Can be used to target every element of an adversary's epistemology
  - Is never decisive, but unlike other resources it is never spent

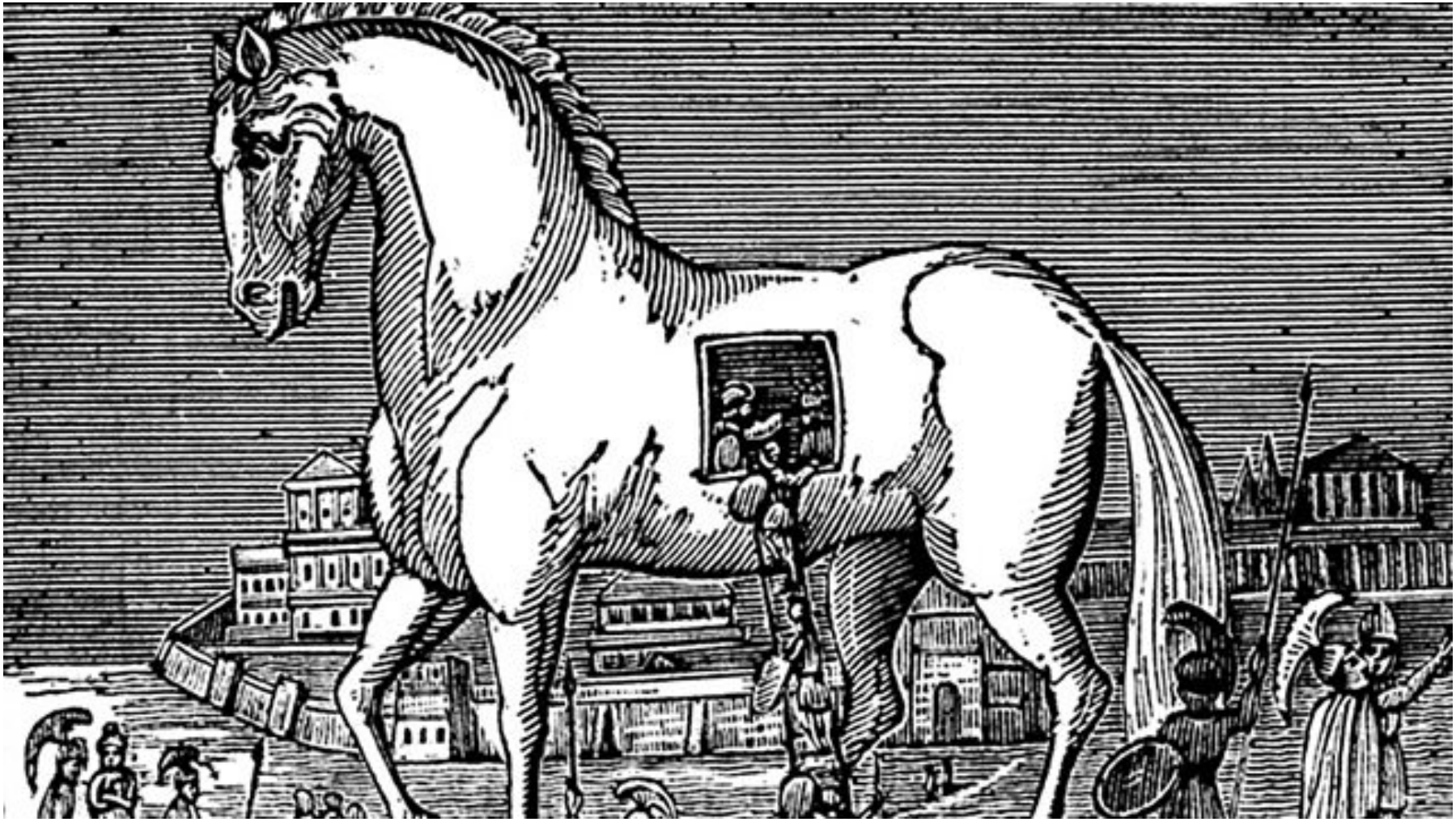
Information as a Weapon



Information as a Weapon

- Information has multirole capabilities
  - A precision guided munition (a DDoS attack on a specific IP address)
  - A cluster bomb (leaflets, pamphlets, tweets / retweets)
  - A dumb bomb (a hijacked website)

Information as a Weapon



Information as a Weapon

Information as a Weapon

Information as a Weapon

Information as a Weapon

Information as a Weapon

Information as a Weapon

Information as a Weapon

Information as a Weapon

Information as a Weapon

- Information Axioms
  - Information is everything; everything is information
  - All human activity has an information quotient
  - All systems move toward greater efficiency;
  - Doing so generates *data* as well as *vulnerabilities*
  - There is no information overload, only data sets you haven't consulted
  - Information management is uncertainty management

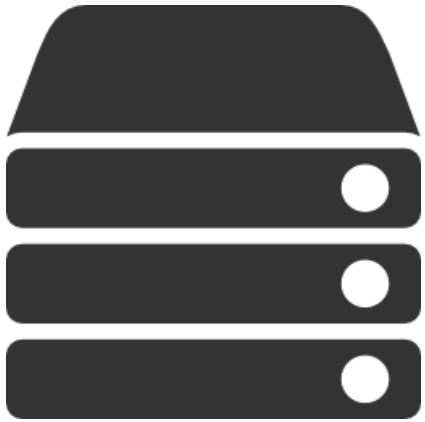
Information as a Weapon

- A Typology of Information Weapons
  - Lethal (Propaganda video)
  - Non-Lethal (DDoS attacks)
  - Kinetic (Stuxnet)
  - Non-Kinetic (Disinformation campaigns)
  - Offensive (Malware)
  - Defensive (Threat intelligence)

Information as a Weapon

- A Typology of Information Targets
  - Repositories: Databases, filing cabinets, minds, etc.
  - Channels: Nodes, networks, cables, servers, etc.
  - Sensors: Humans, algorithms, devices, etc.
  - Intangibles: Trust, authority, reputation, knowledge, etc.

Information as a Weapon



Hardware

Software

Wetware

In Practice

Information as a Weapon

- Information Warfare in Practice
  - Target selection
  - Target scoping
  - Target surveillance / reconnaissance
  - Disinformation
  - Jamming
  - Sabotage

Information as a Weapon

- Effects-Based Operations
  - A mindset and operating philosophy that looks to achieve specific outcomes using multiple approaches
    - Achieve information superiority
    - Leverage strategic / operational advantages
    - Generate a psychological impact
    - Measure first, second, third order effects
    - Measure adaptation / response mechanisms
  - Find the organisation's centre of gravity, the source of its advantage, and look to take it out

Information as a Weapon

- Toolkit
  - Anonymous accounts for all major internet platforms
  - A modern browser (Chrome, Firefox)
  - Knowledge of internet standards
  - A feed aggregator
  - Knowledge of basic / advanced search operators
  - Alert tools
  - Data collation frameworks

Information as a Weapon

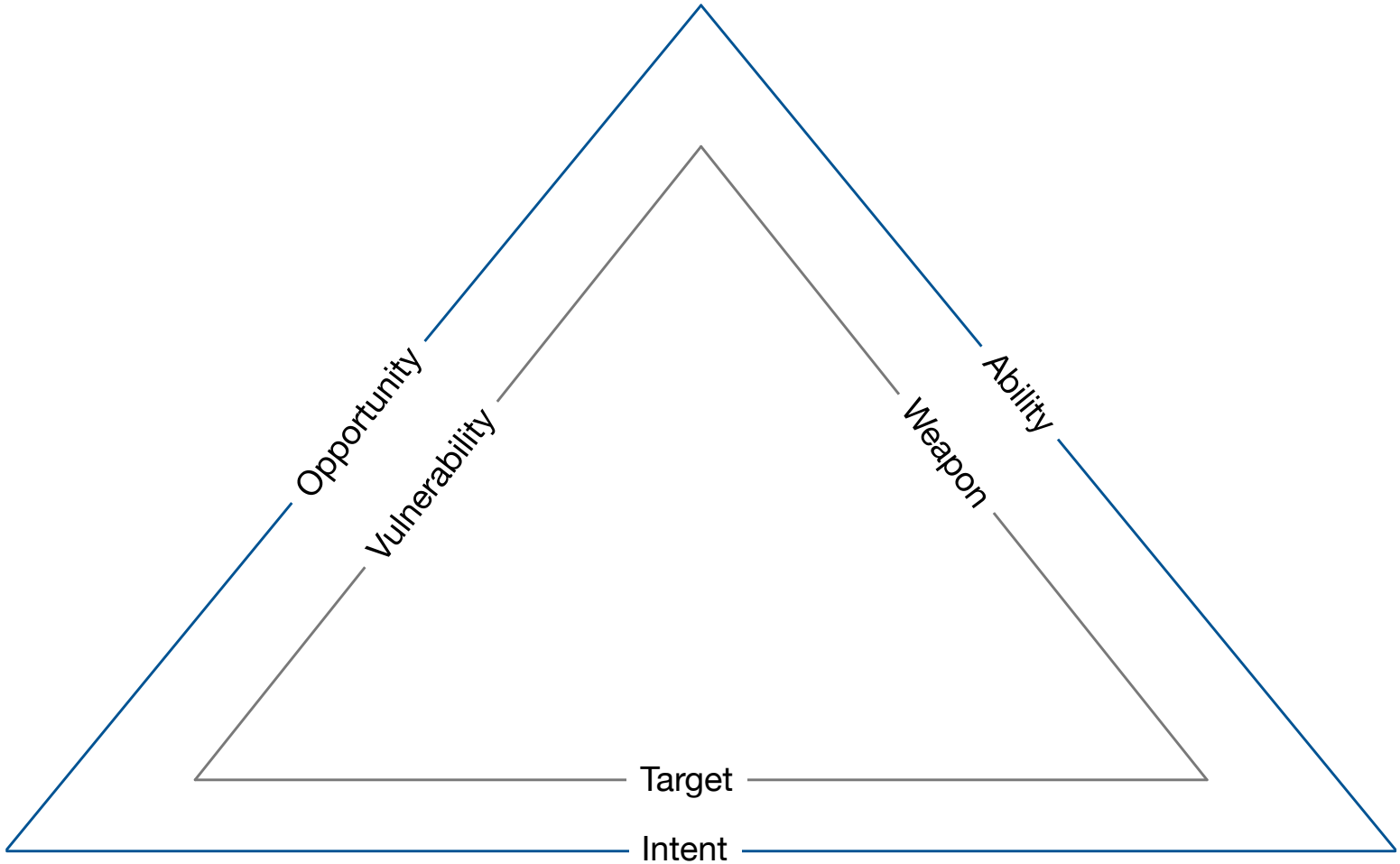
Information as a Weapon

- Your data collection efforts should cover the following domains:
  - Organisational: Data pertaining to an organisation's mission, objectives, etc.
  - Operational: Data pertaining to how an organisation works
  - Informational: Data pertaining to use and management of information
  - Technological: Data pertaining to the use and management of IT
  - Cognitive: Data pertaining to how an organisation and its staff think

Information as a Weapon

Requirements			
Target	**Audience**	**Narrative**	**Concealment**
• To define scope • To measure impact • To determine success	• To amplify the threat • To execute the attack • To determine the appropriate means of deception • To communicate success	• To rationalise your attack • The means by which you will deceive • The means through which you will deny	• To plan your approach • To cover your tracks • Digital alibis • Physical alibi

Information as a Weapon



Information as a Weapon

1. Target Selection

- Objective setting: What / why analysis
- Key intelligence topics / questions
  - Identify and prioritise your intelligence needs
  - If you don't know what you're looking for, you won't find it
- Identify assumptions and hypotheses
- Build your keyword list and data collation frameworks
- Ends / means analysis (is it possible, is it legal)

2. Target Scoping: Organisations

- Profile the organisation's:
  - Mission, mandates, objectives
  - Structure, hierarchy, lines of control
  - Technical infrastructures via DNS / IP / trace tools, etc.
  - Use collation frameworks to organise your efforts

Information as a Weapon

- Organisational Scoping Tools
  - IP / Domain Check Tools
    - http://www.tcpiputils.com
    - http://www.yougetsignal.com
    - http://whois.domaintools.com
    - http://website.informer.com
    - https://www.cvedetails.com
  - Organisational Reviews
    - https://www.glassdoor.com

2. Target Scoping: Organisations

- Use the Five Architectures model to organise your efforts
- Note down any reflections, vulnerabilities as you do so
- Establish and maintain your source index
- Capture, record your work for auditing and accountability purposes
- Develop a systems map; what connects to whom and vice versa
- Leave no stone unturned

2. Target Scoping: Human Beings

- Profile and aggregate data on the organisation's staff
  - Roles, responsibilities
  - Bios, personal details
  - Social media accounts
  - Relationships
  - Interests
  - Publications
  - Contact details

2. Target Scoping: Human Beings

- Aggregate target data using:
  - Social media accounts (Facebook, Instagram)
  - Official, personal photos
  - Username / account name tools
  - Email discovery tools (e.g. Email Hunter)
  - Search operators and general search engines

Information as a Weapon

- Human Scoping Tools
  - People Search
    - http://recruitin.net
    - www.linkedin.com
    - www.facebook.com
  - Reverse Image Search
    - https://yandex.com/images
    - https://images.google.com
  - Email Discovery
    - https://emailhunter.co
    - https://inteltechniques.com/OSINT/email.html

3. Target Surveillance

- Identify information and communication channels
- Automate the collection of data using:
  - RSS feeds / aggregators (e.g. Feedly, Inoreader)
  - Social media monitoring tools (Tweetdeck, Hootsuite)
  - Bridging tools / workarounds (e.g. RSS Bridge)
  - Alert tools (Google Alerts, Queryfeed)

Information as a Weapon

- Surveillance Tools
  - Feedly - http://feedly.com
  - Queryfeed - https://queryfeed.net
  - RSS Bridge - https://bridge.suumitsu.eu

4. Disinformation

- Measure an organisation's vulnerability to disinformation
  - Generate fake profiles, accounts; invite staff to connect
  - Conduct misinformation campaigns; see if analysts pick up on these
  - Generate and circulate fake documents
  - Low volume, targeted emails; high-volume mass deception
  - Test the system in moments of crisis and vulnerability (its not fair, but…)

Information as a Weapon

- Document Spoofing
  - Use search operators
    - “@example.com” filetype:pdf
    - Contracts site:www.example.com filetype:pptx
    - “John Smith” Biography filetype:doc OR filetype:docx
    - Etc.
  - PDF to Word Converter
    - www.freepdfconvert.com/pdf-word

Information as a Weapon

5. Jamming

   - Distributed denial of service attacks
   - Compromise, control, closure, suspension of communications channels

6. Sabotage of information systems

   - Destruction of information systems
   - Deletion of data
   - Access denial
   - Use of malware, zero-day exploits, etc.

7. Analysis and Reporting

- Analyse the findings of your audit: what, so what, now what?
- Do your assumptions, hypotheses still stand? If not, why not?
- What blind spots have you identified over the course of your work?
- What targets, vulnerabilities, attack vectors have you identified?
- How would you exploit them?

Conclusions

Information as a Weapon

- Wrapping Up
  - Everything is relevant; ignore nothing (at least to begin with)
  - The longer you look at something, the more value it has
  - Follow the clues
  - Think like your adversary
  - Ignorance is bliss, as long as you're ignorant
  - Document your work

Information as a Weapon

- Your Weakest Link
  - Your security is only as good as your weakest link
  - Your weakest link is invariably a product of:
    - Ignorance
    - Arrogance
    - Wilful blindness
    - Poor risk management
    - A failure of imagination
  - Each of these sources of failure has an informational component

Information as a Weapon

- Countermeasures
  - Awareness and education
  - Capability enhancement
  - The right toolkit
  - Resilience, redundancy
  - Learn, adapt, reflect, repeat
  - Paradox management

Thank You

Chris Pallaris
Director

i-intelligence

+41 (0) 43 243 3849 | Skype: chrispallaris | c.pallaris@i-intelligence.eu

www.i-intelligence.eu | @i_intelligence