


AIPIO
2012 National Road Show

Counter Intelligence: using the
forgotten intelligence



© 2012 M. J. Dever 1

Outline


Session 1 Contemporary CI

Session 2 Hostile Intelligence Gathering

Session 3 Designing & Making the Case for a CI Programme

Session 4 Technical Security


Concluding remarks



© 2012 M. J. Dever 2

Buzz Words

- Intelligence
- Counter intelligence
- Counter espionage
- Espionage
- Business intelligence
- Competitive intelligence
- Industrial espionage
- Economic espionage
- Corporate intelligence




© 2012 M. J. Dever 3


Intelligence

Definition


- "Information that has been analyzed and refined so that it is useful to policymakers in making decisions".



Intelligence Cycle




Source: NZSIS



© 2012 M. J. Dever 4

Session One


CONTEMPORARY CI



© 2012 M. J. Dever 5


Counter Intelligence

- **Offensive (CE)**
- **Defensive**
 - Counter hostile intelligence collection by adversary
 - HUMINT
 - SIGINT
- **Forgotten ?**
- **CI ≠ Protective Security**




© 2012 M. J. Dever 6

Change

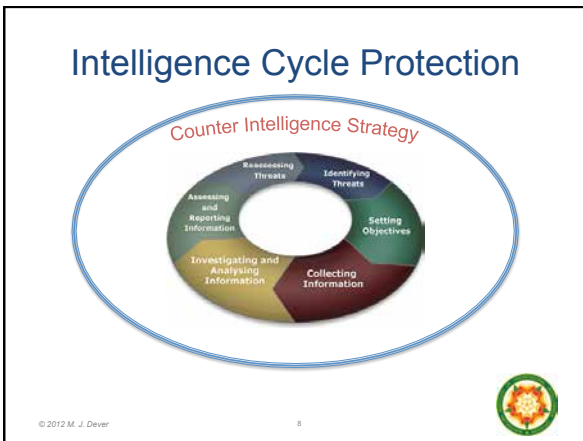


1928 - 2011

- *“The biggest mistake we could make would be to miss the changes”*
 - Glenn Whidden (1990)
- **Changes to:**
 - Adversary capability
 - Technology



© 2012 M. J. Dever 7



Information

That:


- Is of strategic or operational importance
- Contains personal details
- Includes trade secrets or IP
- Is commercially sensitive
- Embarrassing

is lost or compromised

When being:

- Processed
- Transmitted (electronically or spoken)
- Copied
- Stored insecurely


- Adversaries/competitors
- Unauthorised insiders and outsiders
- Media
- Regulators



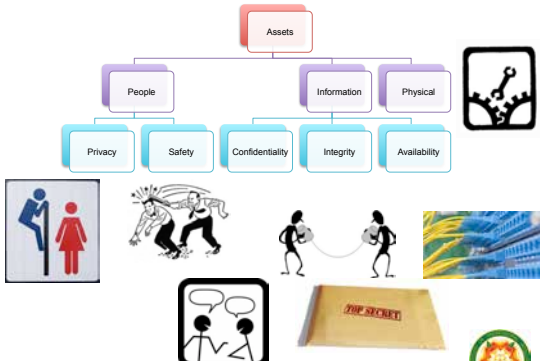
© 2012 M. J. Dever 9

CI Survey Process

- ID Assets
- Threat assessment
- Vulnerability
- Asses risk (SRA)
- Identify and analyse options
- Choose measures
- Write operational requirements
- Implement
- Monitor
- Review



© 2012 M. J. Dever 10



© 2012 M. J. Dever 11

CI Adversaries



EAVESDROPPING
He knows about your secrets!

- FIS
- Organised Crime
- Corporations
- Individuals
- Groups
- Media



© 2012 M. J. Dever 12

Session Two

HOSTILE INTELLIGENCE GATHERING



© 2012 M. J. Dever 13



* Open source (OSINT)
 * Covert
 Human (HUMINT)
 Signals intelligence
 Technical Surveillance



© 2012 M. J. Dever 14

Covert Collection



Hey boss, I'm not sure our covert surveillance is real covert any more.

- Means to an end
- Leisurely
- Legal ?
- Ethical?



- Adversary needs:
 - Access
 - Time
 - Money



© 2012 M. J. Dever 15

Methods

HUMINT

The ENEMY is listening

No wants to know what you know
KEEP IT TO YOURSELF

Swann
Advanced security made easy™
plug&playsecurity

RemoteCam™
Video Camera & Recorder
DVR-410™

- Covert surveillance
- 70ft x 40ft video resolution
- Great color viewing during the day
- 4GB memory expansion
- MicroSD Card

Covert surveillance has never been easier

Technical Collection

© 2012 M. J. Dever 16

Session Three

DESIGNING & MAKING THE CASE FOR A CI PROGRAMME


© 2012 M. J. Dever 17

The Problem
(Threats to confidentiality)

Awareness of the threats

© 2012 M. J. Dever 18

Risk Assessment




High Impact
Low Probability

High Impact
High Probability

Low Impact
Low Probability

Low Impact
High Probability

- Threat
- Vulnerability
- Impact (Business Impact Level)



© 2012 M. J. Dever 19

Risk Acceptance & Tolerance

Isn't that just typical?








© 2012 M. J. Dever 20

Threat Assessment

- Basis for smart security decisions
- Threat is a matter for intelligence



	RECENT		CURRENT		FUTURE		CROSS
	Low	High	Low	High	Low	High	
CAREEN	Medium	Medium	High	High	V High	V High	Common
V BRIG	Low	Medium	Medium	High	High	V High	V High
BRIG	Low	Low	Medium	High	High	High	V High
MEW	V Low	Low	Low	Medium	High	High	
LOW	V Low	V Low	Low	Medium	High	High	
V LOW	High	V Low	V Low	Low	Medium	Medium	
NO	High	High	V Low	V Low	Low	Medium	
NO	V LOW	LOW	MEW	BRIG	V BRIG	CAREEN	



© 2012 M. J. Dever 21

Targets

- Any one with influence, money, power or access to valuable, sensitive or classified information.....
 - Holders of High Office
 - Senior executives (public & private)
 - Celebrities, Royalty
 - Law enforcement officials
 - Lawyers
 - Spouses, neighbours



© 2012 M. J. Dever 22

Motives




- Economic crime
- Organised crime
- Competitive intelligence
- Corporate espionage
- Disgruntled or issue motivated
- Terrorism
- Extortion/harassment
- Internal intrigue
- Media snooping
- Personal privacy invasion/stalking




© 2012 M. J. Dever 23

Capability

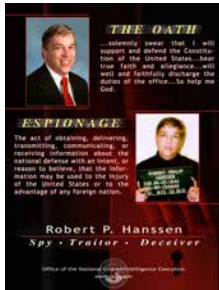
- Time
- Access
- Money





© 2012 M. J. Dever 24

Insider Threat



© 2012 M. J. Dever

25

Vulnerability Assessment



Who will be the first to test your security measures?



© 2012 M. J. Dever

26

Counter Intelligence Strategy

- Key Elements**
- Senior management endorsement
 - Awareness program
 - Compliance
 - Protective security
 - TSCM surveys




© 2012 M. J. Dever

27

Session Four


TECHNICAL SECURITY



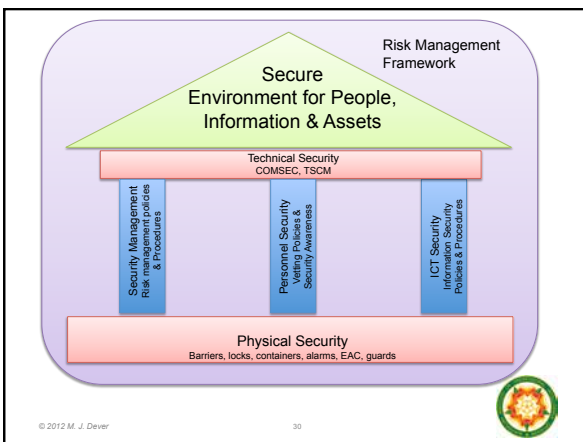
© 2012 M. J. Dever 28

Technical Security

- Measures taken to prevent, deter, and detect intelligence gathering by electronic, electromagnetic, oral, visual and other means
- Technical security is NOT ICT security






© 2012 M. J. Dever 29



Eavesdropping


- **Direct (or acoustic)**
 - Airborne
 - Structural
- **Assisted**
 - Listening devices
 - Communications monitoring



© 2012 M. J. Dever 31


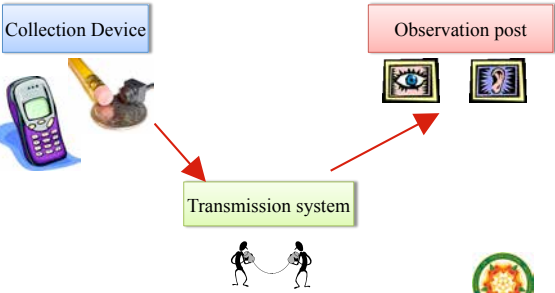
Technical Surveillance Threats

- **Listening devices**
 - Wired
 - Wireless
 - Esoteric
- **Imaging devices**
 - Visible
 - Invisible
- **Tracking devices**
 - Passive
 - Real time
- **Interception**
 - Telephone
 - Fax
 - Keyboard loggers



© 2012 M. J. Dever 32

Basics of Technical Surveillance



© 2012 M. J. Dever 33

Visual Surveillance



© 2012 M. J. Dever 34

MINI-cool-gadget-WHOAS-1.com



Analogue to Digital




© 2012 M. J. Dever 35

3G
4G
WLAN




Interception

- Telephone systems
 - Wired
 - Analogue
 - Digital (VOIP)
 - Wireless
 - Cordless
 - Cellular
 - Fibre
- Two way radios
- Intercommunications




© 2012 M. J. Dever 36



Tracking

Enabled by integration of the navigation, location & social networking services, a person can be tracked from a mobile phone using a service like LBS. The service can be used for a variety of purposes. One of the most common uses is for tracking a person's location. This can be used for a variety of purposes, including tracking a person's location for safety or security purposes.

© 2012 M. J. Dever 37



Evolving audio threats

1920's 1970's Now

© 2012 M. J. Dever 38



Evolving video threats

1962 Now

Camera with 2.4 GHz Transmitter

Medius

© 2012 M. J. Dever 39




TSCM Surveys

Definition

- A systematic physical, electronic and visual examination of a physical item or place by a *qualified specialist* in order to detect technical surveillance devices, technical security vulnerabilities and related physical weaknesses

Protocol

- SRA
- Physical search
 - Vulnerability ID
 - Audio conduction tests
- Electronic search
 - Electromagnetic spectrum
 - Communications systems
 - Building wiring systems and elements
- Anti tamper



© 2012 M. J. Dever 40

Needle in a Haystack?





© 2012 M. J. Dever 41

TSCM Equipment

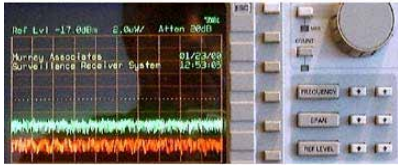




© 2012 M. J. Dever 42

TSCM Specialist

Instrumentation is nothing...



without the right reflection in the screen.



© 2012 M. J. Dever

43

“There are fine cigars and cheap cigars,
but there are no fine cheap cigars”

Winston Churchill



© 2012 M. J. Dever

44
