Intelligence Preparation of the Cyber Environment

Rob Dartnall | Director
– Cyber Intelligence
Rob Dartnall
Director – Cyber Intelligence

Rob is a CREST Certified Threat Intelligence Manager (CCTIM) and Cyber Intelligence Director/CEO of Security Alliance - a Bank of England/DNB/HKMA certified Cyber Threat Intelligence provider under the CBEST/Tiber/iCAST frameworks. With specialist interest areas of Insider Threat and Nation State Fusion Warfare, Mr Dartnall has unique experience and insight into the threat landscape. In his role as the Associate Director of Cyber Threat Intelligence to Gartner, Rob and Security Alliance are the global providers of Threat Intelligence services to Gartner consulting.

From a conventional Military Intelligence background Mr Dartnall has been creating cyber threat assessments and building intelligence teams and testing programs for some of the largest organisations in Europe, North America, the Middle East and Africa.
Rob Dartnall  
**Director – Cyber Intelligence**

Rob is a CREST Certified Threat Intelligence Manager (CCTIM) and Cyber Intelligence Director/CEO of Security Alliance - a Bank of England/DNB/HKMA certified Cyber Threat Intelligence provider under the CBEST/Tiber/ICAST frameworks. With specialist interest areas of Insider Threat and Nation State Fusion Warfare, Mr Dartnall has unique experience and insight into the threat landscape. In his role as the Associate Director of Cyber Threat Intelligence to Gartner, Rob and Security Alliance are the global providers of Threat Intelligence services to Gartner consulting.

From a conventional Military Intelligence background, Mr Dartnall has been creating cyber threat assessments and building intelligence teams and testing programs for some of the largest organisations in Europe, North America, the Middle East and Africa.
Methods
- Hypothesis generation & hypotheses testing
  - Act
- Scenario generation
  - Crisis of instability
    - Breaking the mood
  - Escalation
    - Neighbors, friends
- Restore M.
  - Call/Intell.
  - DJOL
- Before the question
  - Network analysis
  - Event analysis
- Terminology

BIAS
- Confirmation bias
- Anchoring
- Groupthink
- Hindsight
- Scope of imagination
- Availability bias
- Misunderstanding

The use of conventional intelligence methodologies in counter threat intelligence

Don't forget the basics

History of & Intelligence Analysis
- Pre Sun Zu
- Sun Tzu
- Released papers
- Major lessons

Where else has it been used successfully?

Introduction to KGB
- Combat SA / Counter
  - Military INT
  - Strategic assessment
  - Targeting / Network analysis
  - Multi-source evaluation & fusion.

MOCO / MO CoA

Confirm content
@ draft slide deck
@ Speak to story
@ find ref material
@ Create examples
@
THE BRIEFEST HISTORY OF INTELLIGENCE YOU WILL EVER SEE...

CONNECTION PLASIBILITY - BASELINE

Social
- Reliance on 5th - Internal Divisions
- Poor cyber security remains

Technology
- Russia decreases Syria - Increases NATO

Military
- Russia controls Syria - Increases NATO

Political
- Country X plays nicely with Vlad

Economic
- Remains stagnant

Russia continues to play upon internal political divisions due to economic stagnation. A political difference. Poor

MURDER BOARD

...are used to aggressively review, without constraint or pleasantries, a problem, assumptions, constraints, mitigations, and the proposed solution.

BACKCASTING - TIMELINE ANALYSIS

OPERATIONAL
- Nation X increases IP collection Ops via proxy

TACTICAL
- Simple Intrusion

STRATEGIC
- Board regulatory authority's state
- Poor messaging
- Media coverage
- Merger collapses

WE, PHARMACEUTICAL COMPANY X, WILL HAVE SUFFERED A SIGNIFICANT BREACH OF IP THIS YEAR, WHICH LEADS TO A FALL IN OUR SHARE PRICE AND THE COLLAPSE OF OUR MERGER.

PERIOD OF TIME
WHAT ARE WE ULTIMATELY LOOKING TO ACHIEVE?

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

“... IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations.”
There are four main steps:

- Define the battlefield environment.
- Describe the battlefield’s effects.
- Evaluate the threat.
- Determine threat COAs
INTELLIGENCE PREPARATION OF THE BATTLEFIELD

- Define the battlefield environment.
- Describe the battlefield's effects.
- Evaluate the threat.
- Determine threat COAs

PESTLE-M

- Motives
- Weapons
- Sequence of Events
- SIG Posts & Flags
- Third Order Effects

360° Understanding of You, The Enemy, & The Environment
“... IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations.”
"...IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations."
DEFINITION

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

“...IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations.”

INTELLIGENCE PREPARATION OF THE CYBER ENVIRONMENT

“...IPCE is a systematic and continuous process of analysing: the means and motives of threat actors; your digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which you will face threats, enhancing your operational resiliency.”
DEFINITION

INTELLIGENCE PREPARATION OF THE CYBER ENVIRONMENT

“...IPCE is a systematic and continuous process of analysing: the means and motives of threat actors; your digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which you will face threats, enhancing your operational resiliency.”

SANS
“It (IPB) needs to be part of rehearsals, simulation, testing and development now.”

CERT-RMM
“The ability of the organisation to achieve its mission even under degraded circumstances.”

Carnegie Mellon University – SEI
“The key to success in defining the virtual environment is to analyse it from an adversarial point of view.”

OVERVIEW
The Business Club

It is believed that the Business Club began their operations in 2009 using the

CERT
RMM

"The ability of the organisation to achieve its mission even under degraded circumstances.”

Carnegie Mellon University – SEI
“The key to success in defining the virtual environment is to analyse it from an adversarial point of view.”

THREAT CHARACTERISTIC

Threat Severity
Active Since
Source

Russia, Worldwide

2009

Emails containing malicious files often pose as invoices, or notifications of tax rebates. Documents contain obfuscated macros which download the payload.

- Once executed, the Dridex malware downloads a set of C2 OP addresses.
- Communication with C2 server is often heavily encrypted with XOR cipher.

SANS
“It (IPB) needs to be part of rehearsals, simulation, testing and development now.”

CERT-RMM
“The ability of the organisation to achieve its mission even under degraded circumstances.”

Carnegie Mellon University – SEI
“The key to success in defining the virtual environment is to analyse it from an adversarial point of view.”

CERT
RMM

"The ability of the organisation to achieve its mission even under degraded circumstances.”

Carnegie Mellon University – SEI
“The key to success in defining the virtual environment is to analyse it from an adversarial point of view.”

CERT
RMM

"The ability of the organisation to achieve its mission even under degraded circumstances.”

Carnegie Mellon University – SEI
“The key to success in defining the virtual environment is to analyse it from an adversarial point of view.”
**DEFINITION**

**INTELLIGENCE PREPARATION OF THE CYBER ENVIRONMENT**

“...IPCE is a systematic and continuous process of analysing; the means and motives of threat actors; our digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which we will face threats, enhancing your operational resiliency.”

<table>
<thead>
<tr>
<th>CERT-RMM</th>
<th>SANS</th>
</tr>
</thead>
<tbody>
<tr>
<td>“The ability of the organisation to achieve its mission even under degraded circumstances.”</td>
<td>“It (IPB) needs to be part of rehearsals, simulation, testing and development now.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT CHARACTERISTIC</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Severity</td>
<td>2009</td>
</tr>
<tr>
<td>Active Since</td>
<td>Russia, Worldwide</td>
</tr>
</tbody>
</table>

**CERT**

“The ability of the organisation to achieve its mission even under degraded circumstances.”

**SANS**

“It (IPB) needs to be part of rehearsals, simulation, testing and development now.”

**CERT-RMM**

“The ability of the organisation to achieve its mission even under degraded circumstances.”

**Carnegie Mellon University – SEI**

“The key to success in defining the virtual environment is to analyse it from an adversarial point of view.”
### Stages of IPB

<table>
<thead>
<tr>
<th></th>
<th>SEI</th>
<th>US Army</th>
<th>SANS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STEP ONE</strong></td>
<td>Determine the voice of the Environment</td>
<td>Define the Operational Environment</td>
<td>Define the Battlefield</td>
</tr>
<tr>
<td><strong>STEP TWO</strong></td>
<td>Determine the voice of the organisation</td>
<td>Describe environmental effects on operations</td>
<td>Define the Battlefield effects</td>
</tr>
<tr>
<td><strong>STEP THREE</strong></td>
<td>Determine the voice of the Threat Actor</td>
<td>Evaluate the Threat</td>
<td>Evaluate the Threat</td>
</tr>
<tr>
<td><strong>STEP FOUR</strong></td>
<td>(3b) Describe use cases</td>
<td>Determine Threat (CoA)</td>
<td>Determine Courses of Actions</td>
</tr>
</tbody>
</table>
4 Stage of IPCE

FULL SITUATIONAL AWARENESS?

**Determine**

- The Operational Environment
- The Threat Scenarios
- The Threat Actors
- Influences on the Environment

**In Layman’s Terms**

Know yourself and your environment, know the bad guys, know what different compromises could look like and understand what could alter or influence all of the above.
SITUATIONAL AWARENESS

"The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status into the near future."

This Situation awareness takes place at three distinct stages:

Level 1: Perception of the elements in the environment

Level 2: Comprehension of the current situation

Level 3: Projection of the future status

- Endsley 2012, p13
"The key to success in analysing the environment is to assess it from the enemy perspective."

— Naval War college
THERE ARE 3 PERSPECTIVES TO CONSIDER

- FRIENDLY FORCES
- NEUTRAL FORCES
- ENEMY FORCES
STEP 1
DETERMINE THE OPERATIONAL ENVIRONMENT
Step 1: Determine the Operational Environment

- My Operational Environment
  - My Internal Network
    - IT Architecture
    - Security Architecture
    - End points
    - etc.
    - DATA!!!
  - My Internal Network
    - Software/Services/Apps/OS
    - Servers
    - Routers
    - etc.

- Outside my Network
  - My Supply Chain
  - Our Social Media
  - Cloud Svs
  - Services (GitHub)
  - Shadows Svs
  - etc.
STEP 2
DETERMINE INFLUENCES ON THE OPERATIONAL ENVIRONMENT
Determine influences on the Environment

PESTLE
- POLITICAL
- ECONOMIC
- SOCIAL
- ENVIRONMENTAL
- TECHNOCAL
- MILITARY

PESTEL
- POLITICAL
- ECONOMIC
- SOCIAL
- ENVIRONMENTAL
- TECHNOLOGICAL
- MILITARY

PESTIPT
- MILITARY
- ECONOMIC
- SOCIAL
- INFORMATION
- INFRASTRUCTURE
- HYS ENVIRONMENT
Step 2: Determine influences on the Environment

**Internal**
- Political
- Economic
- Social
- Infrastructure
- Information
- Physical Environment
- Time
- Strategy (Business and IT)
- Governance, Audit
- Legal

**External**
- Political
- Military
- Economic
- Social
- Infrastructure
- Information
- Supply chain
- Physical Environment
- Legal

**Influence / effects**
- Geo and Local - Brexit or data sharing
- Military conflict C&E
- Local and regional
- Social norms & views change
- Telcos / Sat? Data Centres
- Extreme weather leads to BC/DR...
- GDPR Cough Cough
STEP 3: DETERMINE THE THREAT ACTORS
Step 3: Determine the Threat Actors

Ultimately you want to know;

Who, what, where, when, how and why.

But how do you answer that...
### Step 3: Determine the Threat Actors – Start big (even bigger than this?)

<table>
<thead>
<tr>
<th></th>
<th>Payment Traffic</th>
<th>Cash Management</th>
<th>Trading Platform</th>
<th>Exchange Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCG</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Nation State</td>
<td>15</td>
<td>20</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>Insider</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>Hacker</td>
<td>12</td>
<td>15</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>9</td>
<td>9</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Corporations</td>
<td>12</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>Terrorists</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>
Step 3: Determine the Threat Actors – Then get more granular

<table>
<thead>
<tr>
<th></th>
<th>Payment Traffic</th>
<th>Cash Management</th>
<th>Trading Platform</th>
<th>Exchange Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCG Y</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>OCG Y</td>
<td>15</td>
<td>20</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>OCG Y</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>APT X</td>
<td>12</td>
<td>15</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>APT Proxy X</td>
<td>9</td>
<td>9</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Hacker Z</td>
<td>12</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>Hacker Z</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>
Step 3: Determine the Threat Actors – What to collect

APT28
AKA: Fancy Bear, Sofacy, Tsar Team, Sednit, Pawn Storm, Group 74, Strontium

Overview

APT28 is widely acknowledged to be affiliated with the Russian government. The group is believed to target sensitive information held by governments, militaries, NGOs, security organisations, and global multilateral institutions. The group's targeting relates closely to the strategic interests of the Russian government. There is a realistic possibility that APT28 receives direction from the Russian foreign military intelligence agency, known as GRU.

The tactics of APT28 display a combination of sophisticated technical expertise and effective social engineering techniques. APT28's tools are suggestive of the group's skills, ambitions, and identity.

The continuous development of the group's TTPs and affiliation to the Russian government means that it is highly likely that APT28 have access to significant levels of resources, both financial and human.

APT28 have been linked with campaigns that include targeting the German Bundestag, TV5Monde, the Democratic National Committee; NATO; cyber espionage campaigns against Georgia, the Caucasus, Eastern European governments & militaries.

In 2016, the group were identified by US authorities and security vendors as the hacking group behind the breach of the Democratic National Committee (DNC) and the World Anti-Doping Agency (WADA). The group has also been associated with targeting the 2017 French Presidential campaign.

More recently, a campaign targeting the hospitality sector has been attributed to APT28. Notably, the group used the NSA exploit EternalBlue as part of its scheme to target Wi-Fi networks to steal credential from business travellers in Europe and the Middle East.

Category

Nation State
STEP 4
DETERMINE THE THREAT SCENARIOS
### Step 4: Determine the Threat Scenarios – MLCoA Vs MDCoA

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Capability</th>
<th>Intent</th>
<th>Threat Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MLCoA: Scenario 1</strong> – An OCG targets the Cash Management to siphon money from the organisation</td>
<td>4</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td><strong>MLCoA: Scenario 2</strong> – An OCG manipulates the xxxxxxx to manipulate stock market prices</td>
<td>4</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td><strong>MLCoA: Scenario 3</strong> – An insider conspires to sell PII and financial information from x asset</td>
<td>4</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td><strong>MDCoA: Scenario 4</strong> – Lazarus Group compromises the Cash Management assets to perform SWIFT transfers involving large amounts of money</td>
<td>4</td>
<td>4</td>
<td>16</td>
</tr>
</tbody>
</table>
WE, PHARMACEUTICAL COMPANY X, WILL HAVE SUFFERED A SIGNIFICANT BREACH OF IP THIS YEAR, WHICH LEADS TO A FALL IN OUR SHARE PRICE AND THE COLLAPSE OF OUR MERGER.
Step 4: Determine the Threat Scenarios – Mapping

1. Reconnaissance
   - Able to identify key employees including software engineers
   - Able to identify VPN login pages
   - Supplier_A User credentials recovered from xxx breach
   - Exploitable vulnerabilities ID’d against a supplier panel using X_tool

2. Staging
   - Job offer spear-phishing completed
   - Software update spear-phishing completed
   - Supplier_A Compromised x 4
   - X_tool successfully runs exploits
   - Active user login granted

3. Exploitation
   - X_RAT uploaded using X_malware loader
   - Video grabbing enabled + keylogger
   - Additional creds captured with x_tool
   - File shares and drives mapped – no role segregation
   - Escalation paths identified using X_tool

4. Control & Movement
   - Escalation attempted in DB
   - Additional creds captured for database administration using X-tool
   - Infrastructure mapped using network X_tool
   - Document folders staged, uploaded and encrypted
   - Initial exfil test passed – WireShark ID’d
   - Data exfil completed based on Wireshark ID

5. Actions On Target
   - Internal email spoof created
   - X_ransomware sent to internal colleagues
   - X_ransomware uploaded to end-point
   - X_ransomware uploaded to DB

6. Persistence & Egress
   - X_ware uploaded to memory
   - Backdoor established
   - PowerShell command uploaded for beacon
Step 4: Determine the Threat Scenarios - Mapping

**Threat actor**
- **Carbanak**

**Threat actor TTPs**
- Identification of employees working on financial payments/technical systems
- Installation of backdoor that can run on start-up. Install additional tools to aid with lateral movement (e.g. Mimikatz, PsExec)

**Outcome**

**Hypothetical outcome:**
- Carbanak compromise xy and performs an illegal transaction to a Carbanak account
- Simultaneously looking to xxxxxxxxxxxxxx for further attacks at a later date

**Testing outcome:**
- Insert xxxxxx into xxxxxxxx (and/or other assets if required)
- Remove cash funds from x

**Attack sequence 1 – XY asset**
- Delivery of spear-phishing emails with attachments containing exploit code

**Distraction Attack**

**Attack 2 – XY asset**
- Duel attack sequence 1) attack into xy and other assets 2) Direct attack on xy
So...where are we?
Situational Awareness

**Determine**

- Perception of the elements in the environment
- Comprehension of the current situation
- Projection of the future status
- Influences on the Environment
- The Threat Scenarios
- The Threat Actors
- The Operational Environment

**Influences on the Environment**

**The Threat Actors**

**The Threat Scenarios**

**The Operational Environment**
Levels of Maturity

Level 1: Perceived
Level 2: Understood
Level 3: Horizon Scan

The Operational Environment

Level 1: Dangerous
Level 2: Baseline
Level 3: Aspirational

The Threat Scenarios
Influences on the Environment
The Threat Actors
Industry, function or region?
WHATS NEXT....

*SANS Says it Best*

“*It needs to be part of rehearsals, simulation, testing and development now.*”
QUESTIONS

With thanks to:

SANS: Use Offense to inform defence. Find the flaws before the bad guys do.
Carnegie Mellon University Software Engineering Institute: Intelligence Preparation for Operational Resilience
US Army and US Marine Corps: Intelligence Preparation of the Battlefield APT2-01.3 / MCRP 2-3A