Back to the Future
Cyber Intelligence and Counterintelligence

Brett van Niekerk
Petrus “Beer” Duvenage
MISCONCEPTIONS

• Myth #1: Cyber intelligence is only about threat feeds
• Myth #2: Cyber intelligence is only about the consumption of information
• Myth #3: Cyber intelligence is cyber espionage
• Myth #4: You need to get the security basics right first
SO THEN WHAT IS CYBER INTELLIGENCE?

Cyber Intelligence

- Cyber threat intel feeds
- Government sources, CSIRT
- Vendor alerts
- Cyber counter-intelligence
- Internal e.g. logs, SIEM etc
- Other sources
SO THEN WHAT IS CYBER INTELLIGENCE?

• Cyber Intelligence is about analysis, not the source of data
  • Examples:
    • Human Intelligence (HUMINT) – human source
    • Signals Intelligence (SIGINT) – signal source
  • Source is important, but does not define it
  • Needs to be actionable
  • Refer to Myths #1 & #2
<table>
<thead>
<tr>
<th>Levels of Intelligence</th>
<th>Strategic</th>
<th>Operational</th>
<th>Tactical</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>General</td>
<td>Industry sector</td>
<td>Company - internal</td>
</tr>
<tr>
<td><strong>Focus</strong></td>
<td>Political, social, behavioral</td>
<td>Adversary campaigns</td>
<td>In the network</td>
</tr>
<tr>
<td><strong>Audience</strong></td>
<td>C-level</td>
<td>Executive management</td>
<td>Sec Ops / response</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Maintain competitive advantage</td>
<td>Avoid disruption</td>
<td>Remediate / recover</td>
</tr>
<tr>
<td><strong>Posture</strong></td>
<td>Proactive</td>
<td>Proactive</td>
<td>Reactive</td>
</tr>
<tr>
<td><strong>Time frame</strong></td>
<td>Far</td>
<td>Near</td>
<td>Immediate</td>
</tr>
<tr>
<td><strong>Types of intel</strong></td>
<td>Estimative, general, scientific &amp; technical</td>
<td>Warning &amp; counter-intelligence</td>
<td>Current intelligence</td>
</tr>
<tr>
<td><strong>Nature</strong></td>
<td>Non-technical, contextual indicators, defence-in-depth approach</td>
<td></td>
<td>Technologies (IDS, SIEM etc)</td>
</tr>
<tr>
<td><strong>Sharing</strong></td>
<td>Public/private partnerships / Cyber security hub</td>
<td>Automated (e.g. feeds – STIX, TAXII, IOC)</td>
<td></td>
</tr>
<tr>
<td><strong>Decisions</strong></td>
<td>Driven by company strategy</td>
<td>Driven by risk-based resource allocation</td>
<td>Driven by restoration / evidence collection</td>
</tr>
</tbody>
</table>

Intelligence and National Security Alliance, *Operational Cyber Intelligence*
THE PREVALENCE OF CYBER INTELLIGENCE

<table>
<thead>
<tr>
<th>Search term</th>
<th>Search term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber intelligence</td>
<td>Cyber threat intelligence</td>
</tr>
</tbody>
</table>

Interest over time

![Graph showing interest over time for Cyber intelligence and Cyber threat intelligence](image)
THE INTELLIGENCE CYCLE

1. Planning & Direction
2. Collection
3. Processing
4. Analysis-synthesis production
5. Dissemination

Finished intelligence
Processed information
Raw intelligence data

Intelligence products
Consumer requirements
Plans

CYBER INTELLIGENCE: NIST CSF

<table>
<thead>
<tr>
<th>TACTICAL</th>
<th>OPERATIONAL</th>
<th>STRATEGIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>Internal</td>
<td>Risk</td>
</tr>
<tr>
<td>PROTECT</td>
<td>Vulnerabilities</td>
<td>Trends</td>
</tr>
<tr>
<td>DETECT</td>
<td>CTI, IOC</td>
<td>Adversary</td>
</tr>
<tr>
<td>RESPOND</td>
<td>CTI</td>
<td>Reputation</td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**CYBER INTELLIGENCE: OODA**


- **OBSERVE**  
  - Detect based on IOCs, behavioural monitoring, vulnerability assessments and SIEM  
  - Prioritise based on threat intelligence

- **ORIENT**  
  - Determine scope/impact based on threat intel  
  - Review in context of other network activity  
  - Attempt attribution / intelligence gathering

- **DECIDE**  
  - Determine immediate steps to respond  
  - Review asset information / instructions  
  - Document all planned tactics for remediation

- **ACT**  
  - Implement remediation & verify success  
  - Review controls, policies & awareness training based on lessons learnt
**Objective:** Reduce MTTD

**Ideal detection window**

---

The planning, establishing, and upkeep of systems with security in mind

Systems added to the Architecture to provide reliable defence or insight against threats without consistent human interaction

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

Collecting data, exploiting it into information, and producing Intelligence

Legal countermeasures and self-defence actions against an adversary

## CYBER INTELLIGENCE MATURITY

### Security Operations Maturity Model (HP Enterprise, 2015)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: Incomplete</td>
<td>Non-existent operational elements</td>
</tr>
<tr>
<td>1: Performed</td>
<td>Meet minimum compliance requirements for security monitoring</td>
</tr>
<tr>
<td>2: Managed</td>
<td>Repeatable operational tasks, meeting business goals</td>
</tr>
<tr>
<td>3: Defined</td>
<td>Well-defined, subjectively evaluated, and flexible operations</td>
</tr>
<tr>
<td>4: Measured</td>
<td>Operations are quantitatively evaluated, continuous review &amp; improved</td>
</tr>
<tr>
<td>5: Optimizing</td>
<td>Implemented operational improvement program tracking deficiencies and lessons learnt drive improvement</td>
</tr>
</tbody>
</table>

### Security Intelligence Maturity Model (LogRhythm, 2015)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: Blind</td>
<td>Capability, organizational characteristics, risk characteristics</td>
</tr>
<tr>
<td>1: Minimally compliant</td>
<td>2: Securely compliant</td>
</tr>
<tr>
<td>3: Vigilant</td>
<td>4: Resilient</td>
</tr>
</tbody>
</table>

|  | MTTD / MTTR |
Cyber Intelligence is clearly critical to Information Security governance, risk and assurance in order to address exponentially increasing threats:

- In 1994, a new threat was discovered each hour.
- In 2006, a threat was discovered each minute.
- By 2012, this had grown to a threat per second.
- By 2014, leaped to over three per second.
- In 2015 nearly seven per second.
- Estimated that 70% undetected.

Current Information Security Approaches + Cyber Threat Intelligence = Gaining the Edge - Shaping the Future ???
What about high-end threats in a complex environment?

High-end threats are increasingly multi-vectored, interlinked and intelligence driven.

What else is needed to ‘Gain the Edge and Shape the Future’?

This part of the presentation briefly examines

- The nature of high-end threats (threat landscape).
- Cyber-security responses in general.
- What Cyber Counterintelligence is and why it is needed.
- As a ‘takeaway’, a CCI-meta model to inform the configuration of organisational Information Security posture.
Multi-vectored intelligence (inclusive of HUMINT) is the name of the game.
ProjectSauron: advanced persistent threat

'ProjectSauron' is a unique 'pattern-less' threat actor responsible for highly-targeted, resource-intensive cyber-espionage attacks against government and research organizations as well as communication and financial companies. Victims have been found in the Russian Federation, Iran, and Rwanda but this is likely to represent the tip of the iceberg.
CYBER COUNTERINTELLIGENCE
– Threat landscape

- Conventional ‘thinking-in-boxes’ no longer holds.
Some recent quotes on threat actors:

- “Nonstate entities, including international terrorist groups and transnational organized crime organizations, will continue to employ and potentially improve their intelligence capabilities, which include human, cyber, and technical means ... These entities recruit human sources and conduct physical and technical surveillance to facilitate their activities and avoid detection and capture.” USA Intelligence Community (2016)

- “distinguishing criminal gangs from nation-state actors (is) a challenge.... Tools and tradecraft become harder to tell apart ... some financial threat groups that we track exhibit traits that look more like state-sponsored APT activity.” Mandiant – FireEye (2015)

- “The primary motivation behind global cyber activity has now shifted from disparate activities carried out by individuals, groups and criminal gangs pursuing short-term financial gain, to skilled adversaries driven by broader agendas.” Crowdstrike (2015)
Some quotes on our responses during the past three years:

• “Regardless of how much we are spending to keep the adversaries out, they are still getting in. If we continue to think of our defences in a check box, technology specific and project-based, nothing is going to change for us ....” HP 2013

• “Cybersecurity experts know well that the perimeter defence approach doesn’t work. All such defences can eventually be penetrated or bypassed. And even without such breaches, systems can be compromised ... when bad guys are already inside the perimeter.” Minister Mahlobo 2015

• “While information security risks have dramatically evolved, security strategies ... have not kept pace ... Most organisations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.” PwC 2013

• “Cyber security goes to the offensive, governments, intelligence agencies, law enforcement and private companies” are increasingly considering “an offensive approach to defend their assets from cyber attacks or to assert its supremacy.” Infosec 2014
**WHY WE NEED CYBER COUNTERINTELLIGENCE?**

- What type of approach do we then need?

- **Five key inter-related requirements**
  - **Defences**: robust and smarter
  - **Offensive**: pro-active identification and engagement of adversaries
  - **Intelligence** at the centre.
  - **Multi-vectored**
  - **Integrated** with organisational DNA and Cyber Intelligence.

- To ‘Gain the Edge – Shape the Future’ we have to go ‘Back to the Future’.

- Counter+ intelligence = counterintelligence.

- Counterintelligence a premise for modelling aspects of our organisational approach.
WHAT IS CYBER COUNTERINTELLIGENCE?

- Counterintelligence's three core **missions**:
  - **Defensive**: prevent, deter and detect.
  - **Offensive**: detect, disrupt, deceive and degrade through active engagement.
  - **Intelligence**: on environment, adversaries and own vulnerabilities.

- A nation-state's CI functions summarised in **D^9**: Defend, Deter, Detect, Deflect, Derail, Disrupt, Deceive, Degrade and Destroy.

- Counterintelligence **methods** range from physical security to offensive ops.

- Since Cyber Counterintelligence is a subset of Counterintelligence it is also multi-vectored.
## WHAT IS CYBER COUNTERINTELLIGENCE?

<table>
<thead>
<tr>
<th>‘CONVENTIONAL’ COUNTERINTELLIGENCE</th>
<th>CYBER COUNTERINTELLIGENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter security and access control</td>
<td>Firewall and validation</td>
</tr>
<tr>
<td>‘Fences’ and CCTV</td>
<td></td>
</tr>
<tr>
<td>Honeypots, dangle, agent/double agent operations</td>
<td>IDS and IPS</td>
</tr>
<tr>
<td>Cover and False flags</td>
<td>Monitor and inspect traffic with complementary aims. IPS is a control tool (‘fence’), IDS is a visibility tool (‘CCTV’).</td>
</tr>
<tr>
<td>All-source CI gathering platforms and services</td>
<td>A honeypot, honeynet and honeywall</td>
</tr>
<tr>
<td>HUMINT network</td>
<td>Network set up to ‘invite’ intrusion or transgression, so that internal and/or external attacker activities, MO and aims can be determined.</td>
</tr>
<tr>
<td></td>
<td>Sock puppets</td>
</tr>
<tr>
<td></td>
<td>Online identity used for purposes of deception and collection.</td>
</tr>
<tr>
<td></td>
<td>Threat Intelligence engines/platforms</td>
</tr>
<tr>
<td></td>
<td>Pool open, deep and dark web sources to analyse threats and trends.</td>
</tr>
<tr>
<td></td>
<td>‘Virtual’ agents</td>
</tr>
<tr>
<td></td>
<td>Penetration of certain hackers forums, closed groups, Darknet</td>
</tr>
</tbody>
</table>
WHAT CYBER COUNTERINTELLIGENCE IS AND IS NOT?

• Cyber Counterintelligence is not?
  ✓ ‘Hacking back’ in a Cyber Wild West.
    - There are very real legal, organisational and practical limitations.
  ✓ Plug-in / add-on service or product.
  ✓ Always a dedicated organisational structure.

• A Cyber Counterintelligence Model provides a starting point to configure and demarcate an organisational approach.
'Dynamic' deception and degrading, generate info

OFFENSIVE

'Hacking back' - disruption, control and manipulation of adversarial systems
Some forms of D&D

DEFENSIVE
Control access, generate info, 'static' deception

Conventional IPS and IDS
Tripwire user accounts
PASSIVE
Deny and ‘direct’ adversary

Feeding of disinformation through
(a) Double agent and/or
(b) Task-configured honeynet

ACTIVE
Engage and ‘control’ adversary

‘Hacking back’ - disruption, control and manipulation of adversarial systems
Some forms of D&D

Intelligence gathering through
(a) Double agent and/or
(b) Task-configured honeynet

Tarpits

OFFENSIVE

DEFENSIVE

Conventional IPS and IDS
Tripwire user accounts
PASSIVE

OFFENSIVE

DEFENSIVE

ACTIVE

Feeding of disinformation through
(a) Double agent and/or
(b) Task-configured honeynet

‘Hacking back’ - disruption, control and manipulation of adversarial systems

Some forms of D&D

Conventional IPS and IDS

Tripwire user accounts

Intelligence gathering through
(a) Double agent and/or
(b) Task-configured honeynet

Tarpits
CCI MODEL FOR AN INTEGRATED APPROACH
CCI MODEL FOR AN INTEGRATED APPROACH
CCI MODEL FOR AN INTEGRATED APPROACH
CCI MODEL FOR INTEGRATED APPROACH

- ‘Theoretical’ model with real practical application.
- Postures will differ.
- Ensures integration and maximise resources.
- Summarised: Bad news can be good news.
CONCLUSION

• Cyber Intelligence and Counterintelligence are interlinked.

• Cyber intelligence and counterintelligence about innovatively applying time-tested practices to the cyber realm.

• Going ‘Back to the Future’ to ‘Gain the Edge - Shape the Future’

• Both relate to strategic, operational and tactical levels across the organization.

• We need to further developed cyber intelligence and counterintelligence in the South African context.

• Ongoing project at the University of Johannesburg.

http://adam.uj.ac.za/csi/CyberCounterintelligence.html
Thank you

Questions / Comments?

Petrus ‘Beer’ Duvenage  duvenage@live.co.za
Brett van Niekerk  academic.relations@isaca.org.za