Operational Templates for State-Level Attack and Collective Defense of Countries

Greg Conti
Bob Fanelli
The views expressed in this talk are those of the authors and do not reflect the official policy or position of IronNet, the US Government, or any of our other current or past employers.
How do we defend organizations, economic sectors, and entire nations in cyberspace?
It feels like our adversaries have strategies, and we have tactics. That’s not very good. I don’t like being in that situation. I don’t like having no strategy.

Jeff Moss
BH USA 2018
Keynote Introduction
MATURE 17+

Blood and Gore
Intense Violence
Strong Language
Nudity
Strong Sexual Content
Use of Drugs and Alcohol

Use of the word Cyber
**Strategic:** Nation-states deciding upon national security objectives and using elements of national power.

**Operational:** Theater commander tying together tactical engagements to support strategic objective.

**Tactical:** Individuals and small units engaging in direct hostilities to defeat enemy forces or seize terrain.
2019: Dim Mak - A Study of the Pressure Points that Could Take Down Cyberspace

2018: What Would You Do With a Nation-State Cyber Army?

2019: Collective Cyber Defense: Towards an Organizational Maturity Model

2017: On Cyber: Towards an Operational Art for Cyber Conflict

2018: Taking Down the Oil and Natural Gas Sector: Into the Mind of the Nation State Threat Actor

2015: Application Military Doctrine to Cybersecurity

2015-Present: IronDefense, IronDome & Iron Shield

2015: Deception for the Cyber Defender

2015: Pen Testing a City


2014: Library of Sparta

2018: Taking Down the Oil and Natural Gas Sector: Into the Mind of the Nation State Threat Actor

2019: Collective Cyber Defense in the Energy Sector

2015: Pen Testing a City

2015: Deception for the Cyber Defender

2015: Applying Military Doctrine to Cybersecurity

2016-Present: IronDefense, IronDome & Iron Shield

2017: On Cyber: Towards an Operational Art for Cyber Conflict

2014: Library of Sparta
The Rout

“a unit that has taken heavy casualties and/or believes itself about to be surrounded, annihilated or overrun by a superior force may suddenly disintegrate into a state of self-perpetuating mass panic”

http://www.youtube.com/watch?v=92gP2J0CUjc&t=1m12s
Defeat in Detail (aka Divide and Conquer)

“...bringing a large portion of one's own force to bear on small enemy units individually, rather than engaging the bulk of the enemy force all at once.”

http://www.youtube.com/watch?v=1jIP55liK5g&t=3m3s

A Tale of Two Teams...

2004 Olympic Basketball Team - USA

2004 Olympic Basketball Team – Argentina

http://www.youtube.com/watch?v=LtopNCH5-qY&t=2m39s
Divide and Conquer Works Really Well When we are Already Divided

- We don’t really even have a team
- We don’t really have offense
- All of society depends on networked information systems
- Medium and small organizations at a severe disadvantage.
- **We will continue being defeated individually, unless we do something**

https://knowyourmeme.com/photos/608525-cthulhu#trending-bar
Defining Collective Defense

• Collective defense is necessary, no company or sector can stand-alone against state-level threats

• Everyone faces state-level threats, either by chance or by deliberate targeting

• Both the private sector and the public sector need to participate or collective defense is impossible

“Collective defence means that an attack against one Ally is considered as an attack against all Allies.” - NATO
Collective Offense

The “Kill Chain” happens here

- Assessment
- Determine desired objectives and end state
- Mission planning and execution
- Target development and prioritization
- Force assignment
- Capabilities analysis

### Instruments of National Power

<table>
<thead>
<tr>
<th>D</th>
<th>I</th>
<th>M</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diplomatic</strong></td>
<td><strong>Informational</strong></td>
<td><strong>Military</strong></td>
<td><strong>Economic</strong></td>
</tr>
<tr>
<td>- Embassies/ Ambassadors</td>
<td>- Military information</td>
<td>- Military operations</td>
<td>- Trade policies</td>
</tr>
<tr>
<td>- Recognition</td>
<td>- Public diplomacy</td>
<td>- Engagement, Security Coop, Deterrence</td>
<td>- Fiscal and monetary policies</td>
</tr>
<tr>
<td>- Negotiations</td>
<td>- Public affairs</td>
<td>- Show of force</td>
<td>- Embargoes</td>
</tr>
<tr>
<td>- Treaties</td>
<td>- Communications resources</td>
<td>- Military technology</td>
<td>- Tariffs</td>
</tr>
<tr>
<td>- Policies</td>
<td>- International forums</td>
<td>- Size, composition of force</td>
<td>- Assistance</td>
</tr>
<tr>
<td>- International forums</td>
<td>- Spokespersons, timing, media and venues for announcements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Navy declares EMS a full-fledged warfighting domain

BY LAUREN C. WILLIAMS • OCT 23, 2018
Global Intelligence Capability
(HUMINT, SIGINT, OSINT, and more)

The science of spying:
how the CIA secretly recruits academics

In order to tempt nuclear scientists from countries such as Iran or North Korea to defect, US spy agencies routinely send agents to academic conferences — or even host their own fake ones. By Daniel Golden
Leverage

Robbeto Graham @ErrataRob · 17 Apr 2018
I'm compiling a list. What ethical dilemmas do we face in the field of infosec?

Tom Cross @decius_
Replying to @ErrataRob
Your government asks you to add a file hash to the anti-virus product you make and tell them if a match appears on one of your customers' computers. They won't tell you what the hash matches, but they insist it's a matter of life and death.

7:25 PM - 17 Apr 2018

Huawei says it would never hand data to China’s government. Experts say it wouldn’t have a choice

Control of the Network High Ground

- Operating a national telecom comes with a position on the global network high ground
- Exclusive power to create and shape the network environment
- Most countries cooperate in good faith
- Uncooperative entities can manipulate the environment for advantage ...or break it altogether
Control of the Foundations of Cyberspace

- Global supply chains for hardware, software, firmware
- Risks of government influence
- Potential for kill switches, back doors, and other “features”
- Opportunity for a wide range of offensive effects
Combined Operations, Large-Scale Effects

- Cut undersea cables
- Disable manufacturing
- Disrupt government and military command and control
- Disable power generation and transmission
- Disable military weapons systems
- Destabilize financial markets and currency
- Cut off cellular, satellite, and internet access
- Use text messages to spread fear
What is a Doctrinal (Threat) Template?

- A model based on known or postulated adversary doctrine.
- Illustrates the disposition and activity of adversary forces and assets conducting a particular class of operation, under ideal conditions.
- Templates are adapted to the given operational environment.
- Depict the threat’s preferred way to use its capabilities and perform the functions needed to achieve its objectives.
Offensive Templates

- Critical Infrastructure Control
- Cyberspace Denial
- Influence Operations and Perception Management
- The Long Game

Defensive Templates

- Basic
- Evolving
- Systematic
- Advanced
- Sophisticated

Hybrid Template

- Defend Forward
Offensive Templates

Organized by threat actor profiles and realistic other possibilities at current level of maturity

Defensive Templates

Tiered based on current and projected maturity
Kill Chain

Operation

Recon ➔ Access ➔ Persistence ➔ C2 ➔ Actions

Recon
- Compromise
- Persistence
- Expansion
- Actions on Intent

TTPs

TTP Graphic by John Lambert, @JohnLaTwC
Campaign
Large Scale Strategy
Operation
Campaign
Kill Chain
Recon Access Persistence C2 Actions
TTPs

TTP Graphic by John Lambert, @JohnLaTwC
Legend

Lines of Effort:
- Information Operation
- Cyberspace Operation
- Physical Operation

Expected Effects:
- “Major”
- “Minor”

Time:
- “Initiate”
- “Develop”
- “Culminate”

Phase 1
Phase 2
Phase 3

Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System

Critical Infrastructure Control

Approach: Achieve a degree of control over adversary critical infrastructure in order to exert power.

- Hold assets at-risk for deterrence purposes
- Conduct shows-of-force
- For economic warfare
- Create disruption for advantage in an armed conflict
Representative Kill Chain Detail View (w/TTPs)

From John Lambert, https://twitter.com/JohnLaTwC/status/1126148047518363649
Cyberspace Denial

Approach: Degrade, deny, disrupt, or destroy the ability to use interconnected networks.

Exert power and induce costs by creating a loss of availability that is more intolerable for the adversary than it is for you.
O2 Cyberspace Denial

**Physical**
- Infiltrate HW Supply Chain
- Recon Undersea Cables
- Infiltrate SW Supply Chain
- Infiltrate Cloud Provider

**Virtual**
- DNS Hijacking
- BGP Hijacking

**IO**
- Obfuscate
- Deny and Excuse
- False Flag

**Phase 1**
- Disrupt Routers via HW backdoors
- Brick Key Systems
- Disrupt Cloud Provider using Insider Access

**Phase 2**
- BGP Hijacking
- DNS Hijacking
- Disrupt Undersea Cables

**Phase 3**
- Monitor for Battle Damage Assessment (BDA)
- DDoS Key Systems
- Manipulate and Disrupt Core Internet Systems

**Key Systems**: Jam SATCOM and positioning services
Influence Operations and Perception Management

Approach: Use cyberspace capabilities as intended, at least from a technical perspective, to persuade, dissuade, deceive, and influence.

Construct and deliver a body of information designed to induce your adversary to willingly act in a manner that furthers your goals.
Information Operations Kill Chain (Zoom)

Inspired by Bruce Schneier, https://www.lawfareblog.com/toward-information-operations-kill-chain, April 24, 2019
The Long Game –
*Death of a Thousand Cuts*

Approach: Achieve long term goals through a series of actions each designed to remain below the threshold of meaningful national response.

 Achieve a win without the adversary recognizing that there has even been a fight.
Staircase of Apathy

An adversary takes a series of steps over time toward their goal.

Small steps aren’t noticed or acted upon.

Large steps are noticed and generate increasingly organized response.

A smart adversary seeks to operate below an apathy threshold to achieve their goal.

... Except when the benefit is so high that an organized response is worth the cost.

Persistent Compromise Key Assets

“Oops, accident”

Repel Outside Tech Presence

Infiltrate Organizations

“Just Normal Competition…”

“All nations spy…” [Pause 6 Months]

“It was Them…”

Espionage: Diplomatic / Political

Espionage: Military R&D

Espionage: Economic IP

Discredit, Deter Dissent

Operational Camouflage and Denial Campaigns

Collect HUMINT

Compromise People

Infiltrate Organizations

Groom “Insider” Actors

Establish Technological Presence and Influence on Adversary

Persistent Compromise Key Assets

Hold at-risk

Test Network Hijack

Network Hijack Ops

Espionage: Economic IP

Operational Camouflage and Denial Campaigns

“Just Normal Competition…”

“All nations spy…” [Pause 6 Months]

“It was Them…”

Create Strategic Ambiguity

Counter Adversary Narratives

Promote Favorable “New Normal”

Recon Ops

Recon Ops

Phases:

Phase 1

Phase 2

Phase 3

O4 The Long Game
H1 Defend Forward

Approach: Reach beyond your national networks to conduct reconnaissance, detect attack preparations, and disrupt attacks, ideally preventing attacks from even taking place.
Defensive Templates by Maturity

Basic
Evolving
Systematic
Advanced
Sophisticated
Organizational Readiness

Interoperability & Information Sharing

Collective Defense

Strong
Moderate
Weak
Basic

- Organizations act as individual islands
- Law enforcement deals with major incidents on limited, case-by-case basis with modest effect
- Limited ability to collect forensic information frustrates response
- North-South sensor coverage
- Suspicion of others in business sector
- Working toward CIS Top 20 controls
- Misaligned incentives
- Primarily signature-based defensive systems
- Government works to defend itself
- Cybersecurity seen as cost center and impediment to business function
What to Expect

• Slow or non-existent government support (First-ever Government interaction?)
• Many companies corporate security will be routed
• Phone calls, post-it notes, and bulletin boards
• Running down halls unplugging systems
• Work stops
• Total disruption
• Weeks/months to recover if isolated incident
Evolving

- Some internal system interoperability
- Need for collective defense understood
- **Limited, but more effective government offensive response**
- General ambivalence toward others in business sector
- **CIS Top 20 controls in place**
- Some external threat intelligence
- Outsourced SOC
- **Slow, relationship-based information sharing**
- Cybersecurity seen as enabler of business function
Level 2 - Evolving

Government

Agency
Intel Agency
Military

Private Sector

Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Company
Systematic

- North-South & East-West sensor coverage
- Member of ISAC
- Occasional trust of others in business sector
- Robust internal security
- **Internal SOC**
- Organizational information sharing and situational awareness
- Sound ability to collect forensic information
- Government response procedures documented
- Signature and some behavioral-based defensive systems
- Professionalized cybersecurity workforce
- Routine internal security exercises, employ threat emulation
- Board actively supports cybersecurity initiatives
- Internal threat intelligence team
Level 3 - Systematic

Government

Private Sector
Advanced

- Aligned incentives
- Collaboration with others in business sector
- **Sector-level situational awareness**
- Participation in sector-level security exercises
- **Sensor coverage extended to ICS systems, supply chain, and organizational ecosystem**
- Sharing of threat information across small, medium, and large organizations
- Inter-organization standard operating procedures
- Councils of CISOs and CEOs address collective cybersecurity
- **Sector-level SOC**
- Behavioral-based defensive systems widely employed
- Joint public/private training
Level 4 – Advanced (Sub-Sector Zoom)
5 Sophisticated

- Regular participation in joint public/private exercises
- Broad, well developed trust between organizations
- Robust, evolving common doctrine
- Government provides rapid effective response
- Automated, adaptive defenses
- **Automated, adaptive requests for government response**
- National-level situational awareness
- Comprehensive system coverage
- Effective, international government response
- Advanced AI/ML defensive systems mature and widely employed

What we aspire to be
Other Models

City
- City Cyber Command
- LE Agency
- Agency
- Company

Corporate Ecosystem
- Manufacturer
- Vendor
- Retail Outlet
- SOC

Ad Hoc Collective
- Government
- Vendor
- Retail Outlet
- Supplier
- Company
Evolving and Applying Templates

- Develop more Offensive and Defensive Templates
  - Corollary: Reverse engineer today’s operations too
- Refine the Defensive Maturity Model and extend the Templates
- Link templates to TTP work, wargaming, scenario development, and training/exercises
- Attackers and defenders will apply specific templates to give them an advantage
What Can Help?

Think in Longer Time Horizons

Public/Private Partnerships for the Defense and Offense

Public/Private Doctrine and Policy for Working Together

Interoperability and NRT Threat Information Sharing

Collective Exercises and Training

Re-think organizational structures and facilities

Automated Response

http://longnow.org/clock/background/
https://www.pondco.com/project/combined-arms-collective-training-facility/
Conclusions

• Collective defense is necessary. Individual heroic response (common today) is the wrong answer
• You can win or lose the battle based on your preparations
• Strong organizational defenses are necessary, but not sufficient
• Trust, teamwork, and a sense of urgency are essential for collective defense
• Military strategy and tactics apply (alarmingly) well to cybersecurity
• The Government might provide some leadership, but it won’t do it for you
• Feedback is welcome, and see the Whitepaper...
Thanks...

- Terry Rice
- H-ISAC Community
- Matt Dolan
- Nick DeTore
- IronNet
- Keith Alexander
- Dave Raymond
- Tom Cross
- Our Black Hat Training Students
Questions

Greg Conti
greg.conti@ironnetcybersecurity.com
@cyberbgone

Bob Fanelli
robert.fanelli@ironnetcybersecurity.com

https://www.youtube.com/watch?v=OWAkNNWo920