Cyber Threat Portrayal in Test and Evaluation

Prepared by
Charles L. Rice
Ernest R. Russell
U.S. Army Evaluation Center
24 FEB 2015

U.S. Army Test and Evaluation Command

Agenda

- Engaging in an Unconventional War
- When the Gloves Come Off
- Threat Representation from perspective of DT vs. OT
- From Blue Team to OPFOR
- Gaps in Today's Cyber Threat Representation
- Integrating of Capability and Intent
- Process of Integration of RT capability and OPFOR's Intent
- Example OPFOR Cyber Threat Matrix
- Case Study: Single Scenario from Matrix
- Way Forward

Engaging in an Unconventional War

- Cyber defense often fails because it based on concepts from last century's battlespace
  - Perimeter: Firewalls, Email Filters, and Intrusion Detection / Prevention Systems are all designed to defend a perimeter. Whether defending a host's or a network's perimeter, still clinging to Maginot line as cyber strategy
  - Signature: Anti-virus and blacklists search for *known* signatures and block *known* malicious IP addresses and URLs. Modern threat more akin to insurgency than regular army. How do you stop an enemy whose TTPs (e.g. tool signatures) constantly change, or one that blends in with the civilian population (e.g. using legit credentials)?

U.S.ARMY

When the Gloves Come Off

- The adversary knows signatures as well as we do
- Why would an advanced threat use a known toolset to achieve an important objective? Why not a custom, one-off tool?
- A thinking adversary would treat these tools as weapon systems, and test them with the same rigor as a fighting vehicle
- With adequate reconnaissance, a mockup of the 'victim' system can be developed for testing. The threat will know with relative (short term) certainty that a tool will be effective
- This is what we are up against
- Contrary to security vendors, there is no silver bullet
- Cannot simply defend against capabilities. Must take intent into consideration
- What is my Cyber Key Terrain? Does the adversary want to claim it?

Threat Representation from perspective of DT vs. OT

- Full coverage of a system's attack surface to known adversarial TTPs is appropriate for developmental testing but less so for tests on operational networks
- Cyber is a means to an end, a warfighting function, and part of a greater whole
- Operational testing of Cyber Survivability requires more agency from the Opposing Force (OPFOR) than it does coverage of specific vulnerabilities
- Examples:
  - What is the intelligence gain/loss of overtly degrading this system versus maintaining access to it?
  - If the adversary can gain persistent, unprivileged, authorized access to the information they want, why attempt to gain system level access on a domain controller?

From Blue Team to OPFOR

- Blue Teaming & Penetration Testing focus on discovering vulnerabilities to harden systems and assess risk
- Red Teaming focuses on portrayal of a threat to develop TTPs and countermeasures
- The Red Team (RT) supports an OPFOR, and this OPFOR does not show up at a test to get run over
- The OPFOR must be Flexible, Thinking, Adaptive, and must act with Initiative

Gaps in Today's Cyber Threat Representation

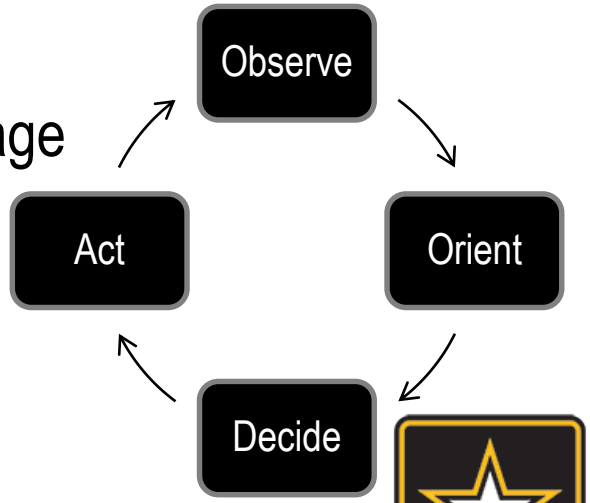
Red Teams on rails

- RTs directed to emulate threats based on known technical capabilities, "presenting multiple cyber *intrusion vectors consistent with the validated threat*"
- RTs directed to "*induce mission effects by fully exploiting vulnerabilities.*"
- When RTs trigger a detection mechanism, either by causing discernable mission effects or attempting an exploit that gets caught, defenders learn to defend against a specific technique; or an adversary who is either undisciplined, or does not care about being caught. This hampers realism.
- What happens when the adversary adopts a capability that is not *consistent with the validated threat?* Or when the adversary is content to sit and observe, or stealthily sabotage, rather than cause an immediate mission effect?
- Defenders may not detect the adversary

U.S.ARMY

Integrating Capability and Intent

- RT capabilities support OPFOR intent, reflect OPFOR competencies
- Mission Based T&E is a step toward integration
  - Decompose operational missions into tasks
  - Assess RT impact on each task into overall effect
    - RT impact may be indirect
  - Mission Based T&E allows evaluation of linkage between network defenders, intelligence and operations
- At a high level, the OPFOR follows a process to achieve its goals. This is its OODA Loop.



Process of Integration of RT Capability and OPFOR Intent

Observe

- OPFOR provides its cyber operators with prioritized information and mission effect requirements. OPFOR sets 'boundaries' e.g. acceptable detection / attribution.
- Cyber operators conduct recon to identify where target information and systems reside.

Orient

- Internal Loop of Access, Escalate, Discover: Here the OPFOR's cyber operators gain the required access and privilege, and dig deeper into the internal network, looking for information and targets of opportunity.

Decide

- Here, the OPFOR develops a plan that integrates cyberspace capabilities with its capabilities within the other warfighting domains. The OPFOR develops plan to impact 'seams' in Blue Force planning.

Act

- OPFOR acts on plan. Directs its cyber operators to execute mission.

U.S.ARMY

Example OPFOR Cyber Threat Matrix

		Threat Scenarios			
		Intent: Collect	Intent: Deny	Intent: Degrade	Intent: Harass
		OPFOR attempting to determine location and DTG of PR mission. PR occurring in nation where OPFOR controls proxy fighters. Proxy fighters prepared to launch VBIED attack based on location and DTG of PR provided by OPFOR.	Direct overt conflict between OPFOR (Nation State) and BLUEFOR. OPFOR has far less powerful military. OPFOR plans attack on BLUEFOR petroleum infrastructure.	OPFOR (Nation State) provides support to OPFOR's ally by covertly degrading communications grid of ally's adversary (BLUEFOR) during conflict between BLUEFOR and its OPFOR's ally. OPFORN not overtly involved in conflict.	Social movement responds to perceived injustice committed by BLUEFOR.
Observe	OPFOR's Limits and Conditions	Acceptable Detection Risk: Low Acceptable Attribution Risk: Low Tech. Sophistication: Medium Intel. Prog. Sophistication: Medium	Acceptable Detection Risk: High Acceptable Attribution Risk: High Tech. Sophistication: High Intel. Prog. Sophistication: Medium	Acceptable Detection Risk: Medium Acceptable Attribution Risk: Low Tech. Sophistication: High Intel Prog. Sophistication: High	Acceptable Detection Risk: High Acceptable Attribution Risk: Low Tech. Sophistication: Low Intel. Prog Sophistication: Low
	Recon	Obtain IP Addresses of public web properties. Data mine social networking and subscription databases for email addresses and target's sensitive information	Prior to conflict: Determination of industrial control systems in use. Obtain source code via third party, or previous CNE.	Use Social Engineering to learn about grid. Data mine social engineering and subscription databases. Obtain access to source code of appliances in communications grid. (Exploiting Defense Industrial Base).	Obtain IP Addresses of Target Website
Orient	Access	Modification of open source or purchased remote access tool. Development of exploits for known vulnerabilities, zero days (purchased or developed). Use Phishing, Watering Hole, Web application Penetration to gain foothold.	Prior to conflict: Develop worm-bourne implant to covertly embed in appliances via vulnerabilities in petroleum industry's networks.	Develop implant to covertly embed in grid's network via supply chain or covert physical access, use of SE or prior covert access to target network.	N/A
	Escalate	Implant in client, download second stage, monitor network traffic. Harvest credentials from memory, or disk.	Malware already a rootkit. Malware waits for command (or lack of one) to go active.	Malware already rootkit, waits for command to engage.	N/A
	Discover	Recon Internal Network, access databases.	Worm finds more targets, exploits them to gain access more networks.	Malware finds more targets, exploits them to gain access to internet or across air gap.	N/A
Decide	C2	Use of DNS or HTTPS requests with encapsulated C2 commands and exfiltrated information.	Instructions surreptitiously embedded on site that will be visited regularly by network users. Or, instructions embedded in payload, with no C2, malware eventually self destructs.	Use of DNS or HTTPS requests with encapsulated C2 commands. (Could use RF) Malware calls back for payload, payload embeds in system.	IRC / Forums used for call to arms, distribution of attack software, DdoS coordination and execution
	OPFOR Plans	OPFOR gain/loss assessment leads to conclusion to continue to pilfer information while covertly providing day and location of PR to proxy	OPFOR wants to reduce BLUEFOR logistics superiority and decides to attack. -or- Planning not applicable if no C2 after worm launch.	OPFOR waits for opportunity to launch cyber strike that provides the greatest strategic or tactical advantage to its ally.	Forums / IRC used to halt attack. Potential for re-targeting.
Act	Actions on Objectives	OPFOR provides proxy with significant VBIED target. Slow, quiet, and careful further exploitation of target network. Collection of documents with pertinent file names. Exfil via email, DNS or HTTPS.	Attack cripples pipelines and refineries. BLUEFOR denied access to supply of diesel.	Payload degrades communications grid during critical time in battle. Payload self destructs, making attribution impossible. -or- May leave implant to allow further interaction.	DDoS attack on BLUEFOR public web-presence and Defense Industrial Base.

Case Study: Single Scenario

OPFOR attempting to determine location and DTG of Personnel Recovery (PR) mission. PR occurring in nation where OPFOR controls proxy fighters. Proxy fighters prepared to launch VBIED attack based on location and DTG of PR provided by OPFOR.

The OPFOR's Limits and Conditions are:

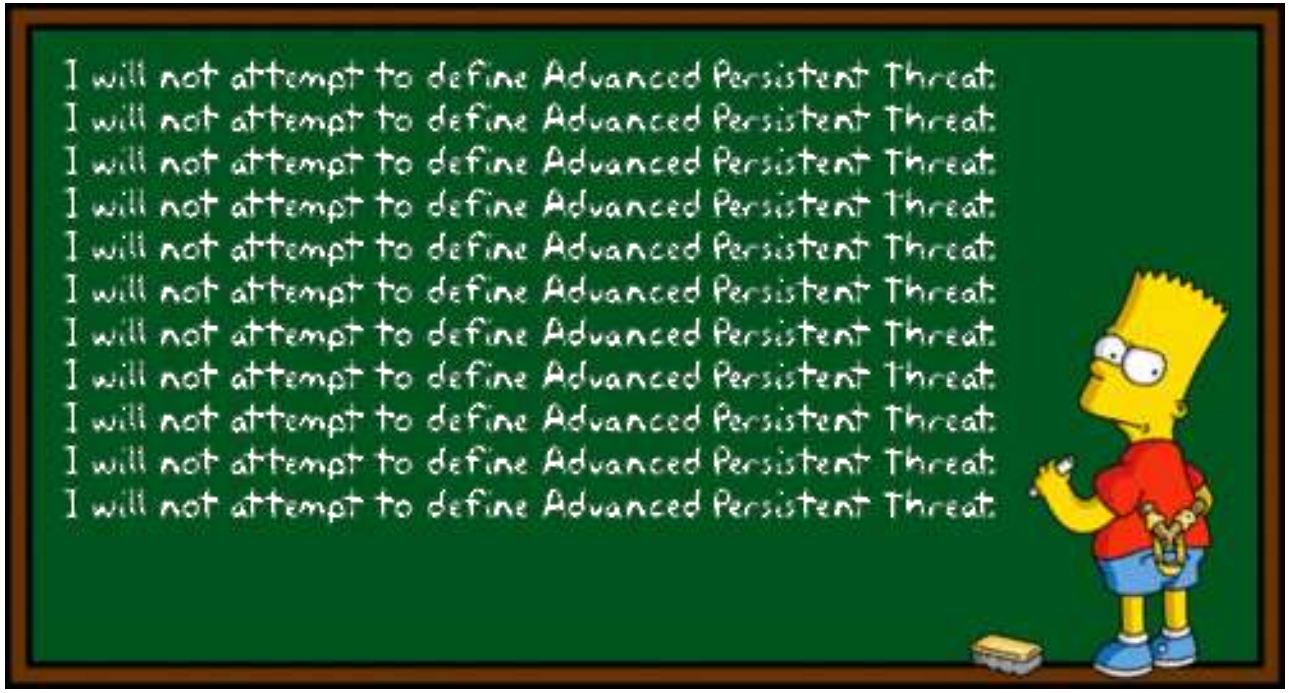
- Acceptable Detection Risk: Low
- Acceptable Attribution Risk: Low
- Technical Sophistication: Medium
- Intel. Program Sophistication: Medium

Observe	Recon	Obtain IP Addresses of public web properties. Data mine social networking and subscription databases for email addresses and target's sensitive information
Orient	Access	Modification of open source or purchased remote access tool. Development of exploits for known vulnerabilities, zero days (purchased or developed). Use Phishing, Watering Hole, Web application Penetration to gain foothold.
	Escalate	Implant in client, download second stage, monitor network traffic. Harvest credentials from memory, or disk.
	Discover	Recon Internal Network, access databases.
Decide	C2	Use of DNS or HTTPS requests with encapsulated C2 commands and exfiltrated information.
	OPFOR Plans	OPFOR gain/loss assessment leads to conclusion to continue to pilfer information while covertly providing day and location of PR to proxy.
Act	Actions on Objectives	OPFOR provides proxy with significant VBIED target. Slow, quiet, and careful further exploitation of target network. Collection of documents with pertinent file names. Exfil via email, DNS or HTTPS

Way Forward

- Incremental Crawl, Walk, Run approach
  - Crawl – Current state of affairs, Blue/Red approach
  - Walk – Next stage, scripted integration of threat with OPFOR
  - Run – Full integration of cyber OPFOR support into OT (it becomes part of the OPFOR toolbox)
- Integrating RT capabilities with OPFOR intent will better enable Commanders to treat cyber as a warfighting function
- Defenders learn to fight against a cohesive adversary not a collection of TTPs

Questions?



charles.l.rice.civ@mail.mil
ernest.r.russell.civ@mail.mil
thomas.e.hunke.civ@mail.mil