SMALL WARS JOURNAL

Cyber Threat Indications & Warning: Predict, Identify and Counter

By ***Scott Swanson****,* ***Craig Astrich*** *and* ***Michael Robinson***

Journal Article | *Jul 26 2012 - 4:59am*

Article Intro

Crime has typically converged with aspects of warfare. This symbiotic relationship further complicates the broad battle-space understanding for early warning vigilance or defensive and offensive maneuvers against nebulous networks and masked relationships of convenience or ideology. The asymmetric cyber domain platform as an adversary's tool to combat a foe unconventionally in a criminal, harassing or potentially devastating non-kinetic manner is no exception. Whether Advanced Persistent Threat (APT) cyber-attacks against the U.S. are used to achieve a military or criminal objective, their encroachment upon political, economic, social, and military networks or infrastructure requires continued insights and operational capabilities in the field to mitigate risk, ensure resiliency, and secure our Nation. This Journal article has converged technology issues, intelligence doctrine, and operational approaches to support the cyber mission and treat hostile actors as any other adversary where threats must to be predicted, identified, and countered in an innovative and decisive manner.

Entities within the U.S. cyber community are edging towards waging more of a counter-cyber-attack campaign to deal strategically and tactically with today's cyber threats over anti-cyber-attack campaigns (Menn, 2012). Anti-cyber-attack is most often associated with active and passive defensive measures used to protect systems from acts. Counter-cyber-attack assumes more pre-emptive offensive strategies to analyze signatures or behaviors and deny the adversary by preventing, deterring, preempting and neutralizing hostile acts and intrusions. This distinction is similar in theory to the anti-/counter-insurgency intelligence approach found in "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan" with regard to where collection efforts are directed and how analytical brainpower is used to improve intelligence relevancy for dealing with a particular issue (Flynn, Pottinger, & Batchelor, 2010).

While cyber defense is required when systems are attacked by single or multiple hacktivists, state sponsored hackers, cyber mercenaries, complex international, politically motivated computer crime or warfare, an aggressive offensive counter-cyber-attack posture and cyber-battlespace awareness by threat operations centers (and associated components) should be a primary task in order to effectively gain and exploit knowledge about the various contexts of operation and distinctions between cyber threat actors, their motives, methods of preparation, attack tree tactics, and intent. The approach requires a hybrid balance of intelligence, counterintelligence and operations that moves beyond analyzing information systems during or after they are attacked. The hybrid approach leverages a broad set of sources and methods to proactively collect and passively detect indicators and signals as early warning discontinuities and threats while there is room for actionable options, as opposed to reactions when options have diminished.

Intrusion Detection: From Reactive to Predictive

Modern cyber-attack warning should concentrate on the identification of indicators as early as possible to augment resilience. This will include examining the dynamic or idiosyncratic features of a future hostile situation that may affect important national interests. This focus, at strategic and tactical levels, will depend less on static potential threat conditions or reactionary responses and more on attempts to isolate the myriad of discrete precursor turning points and discontinuities to identify, track, and reduce the security threat(s). Traditionally, responses to attacks such as those described by the term Advanced Persistent Threat (APT) have focused on identifying indicators within a network to isolate and stop a campaign. Examination of the turning points prior to the launch of an attack is much less common.

Mitigating surprise by assessing such threats can require intensive, process oriented, rigorous analytical work supported by information collection, and coupled with creativity and diverse predictive outlooks. This remains true of most persistent problems that are not simply a focused impending event or responding in a reactionary manner. As such, a key resides in building a spectrum of plausible futures based on vision-based planning that blends information (All Source Intelligence), intuition, and thoughtful judgment to establish and link viable predetermined event- and wild-card scenarios to one another as broadly as possible. Specifically, scenario planning for this effort can leverage a futures warning technique used for medium to long-term strategic analysis, planning, and risk mitigation.

This methodological approach, based largely on works in Strategic Warning, Estimating and Forecasting, and Indications and Warning, can establish viable scenarios and the ability for competing hypothesis so the threat analyst can try to determine relevancy or irrelevancy as evidence of malicious or suspect indicators are identified.

Monitoring indicators across a continuum can nullify some scenarios or hypotheses and illuminate trending towards more viable potential outcomes in a more predictive manner for early warning. Techniques such as “Competing Hypothesis” (Heuer, 1999), Scenario Analysis or the introduction of War Gaming exercises are recommended. At the same time they can provide more tell-tale signs of attackers for more effective (and widely correlating) find and fix targeting objectives.

Creating the Early Threat Warning Framework

Cyber threats can be treated in the same manner as many other discrete or cloaked attacks where the primary focus as defense is on knowing the enemy- his intentions, capabilities, and motivations. Earlier Defense Intelligence Agency analytical frameworks by Cynthia Grabo (2004) and Jonathan Lockwood (1996) can contribute to early cyber threat warning and predictive threat analysis.

Preparations for both cyber and physical attacks in asymmetric conflict consider the differing capabilities and sophistication of hostile actors, the distributed social networks that enable their activities, support, and sustainment, the platform, and the messaging (direct or mediated) that resonates to the point of inciting action on the part of the actor/attacker (such as in the recurring case of Anonymous).

The following framework leverages some elements of Lockwood’s 12-step Analytical Method for Prediction (**LAMP**); however, deep Problem Identification can be effectively assessed through the [Art of] Design framework, taught at the US Command and General Staff College School of Advanced Military Studies.

1. *Problem Identification: Determine the Issue*

The first stage of an effective early warning is in knowing what the problem is, its drivers, and the assumptions that can be made. This requires understanding both the target of the attack and the mechanism by which it is launched. The goal may be to exfiltrate data, alter existing data, transfer money, or reduce the availability of a system. An exploit may be leveraged against identified vulnerabilities in which one can understand eminent risks, or it may be a zero-day attack, where the actual mechanism is unforeseen. In any case, the actual problem must be well-formulated and broken down into component parts so potential adversarial actors can be identified and understood. From that point, probability of intentions, capabilities, and likely actions can be established that characterize the threat to vulnerabilities of access, disruption, denials, corruption, theft, or the destruction of information resident in computers and the systems they reside on. Collecting and sharing of this information can be facilitated through government agencies as well as through industry partners through the U. S. Department of Defense's Defense Industrial Base.

2. Identifying Potential Actors

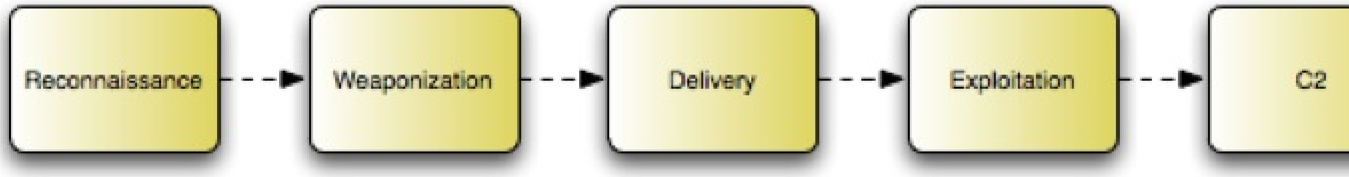
Attribution of attacks back to specific actors has been challenging. Cyber attackers with cloaked identities, proxied network connections or bulletproof hosting services, and operating bases in remote locations create clear issues for analysts in recognizing an actor and associating him with a nation state attack or a non-state individual or group. Advanced studies of how each potential actor identifies and perceives the opportunity for attack is performed by issuing full spectrum collection operations against the threat activities, plans, and intentions.

Cyber profiling through social media analysis (and Cyber-HUMINT/CI) can play a critical role in the advance appreciation of foreign influence and strategic messaging from the standpoint of being able to better assess the messenger, message, and intended audience. To this point, warnings and signals of individual participation in social media based on profile of communication and performance traits, the resources they have available, the methods they would use, objectives, and their motivation (gun, bullets, and trigger model) add to the datum pointing towards particular scenarios. This may include:

1. Map of the potentially hostile environment.
2. Identifying individuals or groups that require monitoring and vigilance.
3. Developing a prioritized list of future targets.
4. Prioritize the importance and impact capabilities of these actors as threats for collection management purposes and risk evaluation.
5. Identifying the actor threats that will likely have access through direct tasking or ideology for a potential Insider Threat.

3. Actor Courses of Action: Viability and Probability

Cyber-attack progression typically follows a "kill chain" cycle as published by Cloppert in 2009. The various phase-gates that occur (in both linear and parallel flows) can be predetermined in many cases towards the eminent attack. Issues which occur to the far left of the kill chain in the Reconnaissance and Weaponization phases, have been difficult to observe, whereas events that occur to the right and start at the Delivery phase can be more easily identified and analyzed because evidence resides on the systems that have been compromised. While it is challenging, identification of actors by their activity in the far left of the chain can lead to an effective countermeasure before an attack occurs—particularly where illicit finance is concerned as inducement, and follow-the-money ("FININT" Financial Intelligence and Counter Threat Finance) procedures can be implemented.



Cloppert’s Advanced Persistent Threat Kill Chain (2009)

4. Determine Scenario Enablement

Adversaries have proclivities towards computer resources and methods according to their preferences, style or training, and resources at their disposal. By understanding their tendencies and technological capabilities or limitations, which can be collected, the adversary can be exploited to the point of understanding intent, motivation, and capabilities. This becomes increasingly complex when actors function in teams to expand their capabilities. This is useful in cyber-attacks, because the skills used to successfully launch an intrusion into a network are different than those used to move laterally through a system and exfiltrate data.

In the cyber community many of these data points can be identified by pre-determined patterns and signals in behavior or emotionally driven sequences. In other cases where they cannot be pre-determined, they can be collected, and therefore should be monitored, tracked, recorded for groups and particular adversary profiles to draw inferences and future intelligence driven responses. This may involve monitoring the activity on specific areas of the Internet such as Internet Chat Relays (IRCs), 4chan.org, Pastebin, etc.

5. Manifested Scenario Focal Events

With no real boundaries established on the Internet, guarding cyber borders from attacks requires conceived multi-layers of defense to implement detection systems that are honed to identify clusters of activities that identify patterns of behavior that show a targeted objective (or mission) is underway. One-off activities may not be a strong indicator of a future cyber-attack and the activities might go unnoticed. When activities, attack points, and methods are clustered together, a pattern can be identified and analyzed resulting in predictive behavior. The defense system must be able to identify an active kill chain “Focal Event” in its early stages to break the event flows to thwart an attack from progressing and identify the attacker or their technique footprint to defend against subsequent occurrences.

6. Create Focal Event Indicators: An adversary prepares for hostilities

Indicators can be catalogued and classified a number of ways that correlate to the observable tactics, techniques, and procedures followed as an attacker progresses towards his end state Focal Event objective of the assault. These pieces of data can demonstrate the presence of activity despite the fact that they may not exclusively represent only activity conducted by the adversary and their sole signature. When combined with behavior, the indicators trend towards a profile.

7. Collect and Monitor through Indicators: Assess Emerging Trends

Analyst teams will collect and monitor identified activities or circumstances that are part of the Cyber Threat actor’s *modus operandi* that correlate as indicators. The indicators may not equate to an actual foreign probe, collection, or attack threat; they can act as a signal to the scenarios and to a general evolution of an occurrence. As the number of indicators in a given situation progress they likely warrant further investigation or collection tasking.

8. Discern the Probable Scenario that is Trending

As indicators point to a particular scenario manifestation, the scenario(s) can be reassessed and further exploited to determine that the development and necessary attributed actions are considered for viability. It is critical at this stage that data analytics are being used to sort through vast amounts of sensor data that may be coming in. The cyber domain as a vast sea will overwhelm integrated multi-source intelligence feeds if they have not been calibrated to detect specific and relevant data points in the system of processing, exploiting, and disseminating (PED process).

9. Readjust for New Manifestations of the Scenario

Change and adjust specific scenarios and their structure elements as more threat signature information is received and analyzed towards the hypothetical solutions to reject the viability of the proposed alternatives when a more substantive alternative scenario outside of the choice set may be occurring.

10. Deception in Indicators

Early warning analysis can produce a number of valid indicators but may also capture deception indicators that have been created to throw off surprise mitigation efforts. Indicators should not just be collected but rather, they should also be monitored further in context and tested to correctly predict an adversary's next move. Further, as a counterintelligence capability, offensive deception activities should be executed to feign weaknesses or to trap the adversary.

11. Mental Model Avoidance: Is it expectation or actuality; theory or current developments?

For every development based on the present indicators, a number of options for action or inaction should be determined by evaluating the micro-situation and assessing whether the occurrence is actually part of the kill-chain flow or if it is a mental model mind-set expectation that could be a feign, false flag, anomaly, or figment of the imagination. Here the OODA Loop decision making model may be of help in examining the actuality of event according to the principals of Observe, Orient, Decide, and Act.

12. Strategic Options Analyzed Against Viable Scenarios

As the scenario occurrence nears fruition, strategic or tactical options can be executed. The options to be executed ideally would have been previously reviewed in an earlier Course of Action (COA) testing and Red Team analytical framework as a reality check to how the major challenge or risk could potentially unfold.

In this final stage, the pre-developed contingency plans would be executed if all efforts towards deterrence, denial, and destruction were exhausted.

Conclusion

Cyber threat security breaches are on the rise globally and this new face of irregular warfare by asymmetric hostile actors, both foreign and domestic, is leading many to believe that terrorists and criminal cartels could in due time recruit significant cyber armies through social media that can permeate network defenses internally and externally. However, defenses much like counter-Improvised Explosive Devices (IED) programs may be more focused towards defeating the "device" or technology, as opposed to directly engaging with the human factors and those who are motivated to use the internet as a weapon. In Flynn's paper (2010), he addresses counter-insurgency intelligence failures when intelligence lacked meaningful substance for insights or action, and when analysts could barely scrape together enough information to formulate rudimentary assessments of critical knowledge gaps.

Cyber warfare is yet another method of conducting war that requires thoughtful analysis of operationalized intelligence for offensive capabilities in tandem with our defensive abilities. In the end, policy makers and analysts should focus less on monikers of war tools/weapons associated with cyber warfare and train its collection and analysis more on the actual or viable perpetrators who either actively conduct the attack or those who motivate others than in how to build walls to prevent breaches from attackers inside and outside "the gates." Failure to do so can be seen as a wartime failure of intelligence, which can be easily averted before disaster. Cyber threat is an issue that can be collected against through aggressive intelligence, and can be predicted through analytical rigor and futures methods. By leveraging the "INT's" in a thoughtful manner towards the actual problems, offenses and defenses can be improved and adversaries can be better identified, deterred and defeated for better outcomes and mitigated surprises.

As Flynn states, "Highly complex environments require an adaptive way of thinking and operating. Just as the old rules of warfare may no longer apply, a new way of leveraging and applying the information spectrum requires substantive improvements—often in the areas of innovative strides—to constantly change our way of operating and thinking if we want to win" (2010).

References:

Cloppert, M. (2009, October 14). "Security Intelligence: Attacking the Kill Chain." Retrieved on June 1, 2012 from the SANS website: http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

Flynn, M. T., Pottinger, M., & Batchelor, P. D. (2010, January). "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan." Voice from the Field. Center for a New American Security. Washington, DC.

Grabo, C. M. (2004). Anticipating Surprise: Analysis for Strategic Warning. University Press of America.

Heuer, R. J. (1999). "Chapter Eight: Analysis of Competing Hypothesis." *Psychology of Intelligence Analysis*. Center for the Study of Intelligence. Central Intelligence Agency. Pp. 95-110

Lockwood, J. (1996). Lockwood Analytical Method for Prediction, DC: JMIC.

Menn, J. (2012, June 18). "Hacked companies fight cyber criminals." Retrieved on June 18, 2012 from the Canada.com website:
http://www.canada.com/technology/Hacked+companies+fight+cyber+criminals/6799367/story.html

About the Authors

Scott Swanson

Scott Swanson is a Defense and Intelligence advisor within Deloitte Consulting LLC's Federal practice. He is a published author and instructor on the topics of special operations, red teaming, critical infrastructure protection, irregular warfare, illicit finance, proxy actors, and intelligence topics. He has supported the community as a cleared professional with his work as an analyst and in the field.

Craig Astrich

Craig Astrich is a Senior Manager Audit and Enterprise Risk Services where he is focused on Technology Risk for Intelligence Agencies within Deloitte's Federal practice. Craig has 17+ years of experience serving a wide variety of Federal (Defense, Intelligence, and, Civilian agency) and Commercial clients. In these engagements he led integrated teams, while developing new capabilities and new service offerings. Prior to Deloitte, Craig served as a Senior Leader at Booz Allen Hamilton for 13 years leading cyber teams across Federal Defense, Intelligence, & Civilian agencies while driving new/emerging capabilities. These capabilities focused on IT Infrastructure, Computer Network Defense (CND), Security Automation, mobile device security, security engineering, and security program management.

Michael Robinson

Michael Robinson is a Specialist Leader in Deloitte's Audit and Enterprise Risk Services. Michael has 15 years of experience in Information Technology (IT) in Federal and commercial sectors with work in computer and mobile device forensics, information assurance, network design, and help desk operations. In addition to working at Deloitte, Michael teaches computer and mobile device forensics at George Mason University and Stevenson University. He recently designed Stevenson's newly accredited Master's Degree in Cyber Forensics. He is currently pursuing a doctoral degree at George Mason University. Prior to joining Deloitte, Michael conducted computer forensic examinations for the FBI in support of counter intelligence and criminal investigations, and was the Chief Information Officer (CIO) for the Department of Defense's Business Transformation Agency.

Available online at : http://smallwarsjournal.com/jrnl/art/cyber-threat-indications-warning-predict-identify-and-counter

Links:
{1} http://smallwarsjournal.com/author/scott-swanson
{2} http://smallwarsjournal.com/author/craig-astrich
{3} http://smallwarsjournal.com/author/michael-robinson
{4} http://lamp-method.org
{5} http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain
{6} http://www.canada.com/technology/Hacked+companies+fight+cyber+criminals/6799367/story.html
{7} http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008