2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Applying Indications and Warning Frameworks to Cyber Incidents

Bilyana Lilly
RAND Corporation
Santa Monica, California, United States
blilly@rand.org

Lillian Ablon
RAND Corporation
Santa Monica, California, United States
lablon@rand.org

Quentin E. Hodgson
RAND Corporation
Santa Monica, California, United States
qhodgson@rand.org

Adam S. Moore
RAND Corporation
Santa Monica, California, United States
amoore@rand.org

Abstract: Despite significant advancements in academia and public policy on identifying, deterring, and mitigating cyber incidents, there is a general discontent among NATO agencies, member states' governments, and intelligence agencies that their strategy against cyber incidents is primarily reactive and implemented *post factum*, rather than proactive and executed before such attacks occur. This issue could be addressed through the design and application of appropriate indications and warning (I&W) frameworks for the cyber domain. Currently, there is a lack of comprehensive understanding and generally accepted practice of how governments and international organizations can apply such I&W methodologies and integrate them with their existing capabilities and processes. A survey of the classic warning methodologies used by the U.S. intelligence community to address a range of non-cyber threats can inform the design of such robust frameworks. These mature intelligence methods can be adapted and perfected to adequately address threats in cyberspace. In this article, we examine some of these I&W frameworks and propose a high-level practical approach to cyber I&W that governments, NATO agencies and the private sector can use to design and structure their prevention, detection, and response mechanisms in order to effectively anticipate and defend against cyber threats. To demonstrate the utility of this approach, we apply it to an actual case: the November 14, 2018 spear-

phishing campaign by Russia's APT29 against U.S. government agencies, think tanks, and businesses.

Keywords: *indications and warning, cyber warning, warning framework, threat intelligence, cyber, I&W, ATT&CK, APT29, cyber threat intelligence*

1. INTRODUCTION

In light of rapidly evolving technology and cyber threat landscapes, increased availability of commodity and modular polymorphic malware, as well as open-source hacking and post-exploitation tools, governments and international organizations face significant challenges in ensuring robust and effective defenses in the cyber domain. While traditional approaches of detecting and mitigating cyberattacks have been successfully applied to protect networks and maintain cyber resilience, these approaches are primarily reactive and retroactive, rather than proactive and implemented in advance of an impending cyber incident.[1] Cybersecurity representatives from governments, international organizations, and the private sector have expressed concern with this method and a desire to enrich it by designing a more forward-looking, practical approach to provide indications and warning (I&W) – or actionable intelligence and monitoring of potential threats – sufficiently in advance to enable the early detection and reaction to cyber incidents before they occur. The ability to design such an approach is hindered by the lack of a commonly accepted definition of cyber I&W, the highly classified nature of the field, and the layers of complexity introduced by constantly changing threats and networks.

In an attempt to address this problem, this research proposes a high-level yet practical strategic cyber I&W approach that governments, NATO agencies, and the private sector can apply to defend against cyber threats. The proposed approach is informed by mature I&W frameworks that the U.S. intelligence community (IC) has developed, refined, and consistently applied to monitor non-cyber threats throughout the Cold War and today. The practices of the U.S. intelligence community serve as an appropriate methodological foundation for a cyber I&W approach that can be introduced across NATO members and agencies, due to the availability of open-source literature and the broad influence of the U.S. IC in both NATO and among other Allied nations.

This article commences by first, outlining the evolution and history of I&W in the U.S.

1 For the purposes of this article, cyber incident is defined as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein." See U.S. Code of Federal Regulations, Title 48, Chapter 2, Subchapter H, Part 252, Subpart 252.2, Section 252.204-7012. Additionally, see CJCSM 6510.01b for a table of Incident Categories.

intelligence community. Second, it examines the existing definitions of cyber I&W and the divergent understanding among scholars and practitioners regarding how I&W can be applied to the cyber domain. As a third step, the research examines classic I&W frameworks for non-cyber threats and recent literature adapting I&W frameworks to cyberspace. Finally, on the basis of identified strengths in the existing approaches, the article offers a general practical approach to cyber I&W that governments, NATO agencies, and the private sector can consider adopting. To demonstrate the practical utility of our proposed approach, the research concludes by applying it to an actual cyberattack: the November 14, 2018 spear-phishing campaign by Russia's APT29 against U.S. government agencies, think tanks, and businesses.

The analysis is based on a mixed methods approach, including an examination of relevant publicly available literature such as articles, books, and reports. The literature consulted was compiled as a result of a systematic literature review of relevant databases including JSTOR, EBSCO, IEEE Xplore, and Web of Science. The research was also informed by a review of primary sources such as national cyber and military doctrines, and speeches by military and government representatives of NATO member states and NATO agencies. The arguments were further shaped and refined by a synthesis of insights gathered through correspondence and discussions with cybersecurity staff of international organizations, the U.S. government, and the private sector. This research is based on open-source literature and, due to the highly classified nature of the intelligence tradecraft, the scope, depth, and detail of the analysis and recommendations is limited. Therefore, this article should be considered as a starting point and general methodological framework of addressing the issue, accompanied by a set of recommendations, which should be adapted and refined further by agencies and decision-makers.

2. DEFINITIONS OF WARNING INTELLIGENCE

The conceptualization of indications and warning provides valuable insights into the evolution of threats and the utility of I&W approaches adopted to defend against them. The overview provided in this section describes the main elements of the I&W concept adopted and employed by the U.S. intelligence community since World War II, outlines variations in the definition of some of the key terms used in I&W frameworks in the cybersecurity community, and concludes by proposing a definition of cyber I&W.

Indications and warning is "an intelligence product upon which to base a notification of impending activities on the part of foreign powers, including hostilities, which may adversely affect military forces or security interests." (Watson, Watson and

Hopple 1990, 594; Grabo 1987, 5)[2] It includes "those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests." (Department of Defense 2013, p. GL-12) Warning intelligence is an analytical process that serves to assess continuously and report periodically on any developments which could indicate that a state or non-state actor is preparing an action which could threaten U.S. security interests and the interests of U.S. allies. It scrutinizes military, political or economic events, as well as other relevant and associated actions and developments or plans that could provide further insight into potential preparations for hostile acts. The analysis is an assessment of probabilities and provides a definitive (positive or negative) or a qualified (high, medium, low probability) judgement about the likelihood of the threat should it be brought to the attention of a policymaker. Warning intelligence is an art that requires understanding and continuous study of the capabilities, culture, history, and biases of potential adversaries. It applies to routine continuous monitoring and in crisis situations (Goldman 2002, iii-3).

In the context of warning intelligence, there is a fine distinction between the terms *indicator* and *indication*. An *indicator* is a theoretical or known development or an action which the adversary may undertake in preparation for a threatening act such as a deployment of forces, a military alert, a call-up of reservists, or the dispatch of a diplomatic communique. An intelligence organization anticipates an indicator's potential occurrence and adds it to a list of items to monitor, which is known as an "indicator list." Therefore, an indicator is a judgment based on collected evidence that an action of concern may happen. Information that an indicator is actually taking place constitutes an *indication*. The purpose of the *indication* is to provide insight into the adversary's potential course of action. Thus, the difference between an *indicator* and an *indication* is one between theory and practice; or expectation and an actual development (Goldman 2002, 3).

In contrast to the U.S. Department of Defense (DoD) and IC, the broader cybersecurity community has a different use of the term *indicator*. In this community, *indicators of compromise* (IOC) is used to refer to evidence indicating a breach in the security of a network (DeCianno 2014). This technical use of IOC is similar to the term *indication* described earlier. Throughout this article, we use the terms indicator and indication as they are defined in the U.S. DoD and IC. Another term, used later in this article, is *Priority Intelligence Requirements* (PIRs), which refers to an intelligence requirement to "focus information collection on the enemy or adversary and the [operational environment] to provide information required for decision making." (Joint Chiefs of Staff 2017)

2 Indications and Warning has also been referred to as warning intelligence or indications intelligence.

Strategic warning does not have a universally accepted definition (Goldman 2002, 3). In its broad sense, *warning* is defined in the U.S. IC as "a notification of impending activities that may, or may be perceived to, adversely affect U.S. national security interests or military forces." (JMIC 2001, 38) It is further defined as "[a] distinct communication to a decision maker about threats against U.S. and allied security, military, political, information, or economic interests. The message should be given in sufficient time to provide the decision maker opportunities to avoid or mitigate the impact of the threat." (DIA Instruction 3000.001, 2014)

I&W has traditionally been focused on monitoring the behavior of potential adversaries on air, land, at sea, and in space. The distributed denial of service attacks on Estonia in 2007 placed cyber operations among the tools of statecraft and necessitated heightened focus on another class of monitoring targets from a relatively new environment: threats emanating in and through cyberspace. Today, warning intelligence incorporates a variety of threats and potential adversaries, both state and non-state actors that can initiate activities harmful to U.S. interests across multiple domains, including cyberspace. This wide spectrum of actors, methods and scenarios is reflected in a broader definition of threats, including any "discernible danger" that can inflict potential damage "to U.S. or allied persons, property or interests that occurs in a definable time in the future." (DIA, Warning Fundamentals, 4)

Considering the gravity of threats to cyberspace, developing the capability to anticipate—not just react faster to—these threats would better position cyber defenders to accomplish their goals. Adapting I&W methodologies to the cyber domain would provide them with the means to do so; yet cyber I&W concepts and frameworks, as well as protocols on how to integrate these into the intelligence tradecraft, are still evolving (INSA 2018, 1; Correspondence with a cybersecurity expert, December 17, 2018). Neither NATO agencies nor the U.S. government provide publicly available comprehensive definitions of cyber I&W, perpetuating divergent understandings of cyber I&W frameworks.

Based on the literature and doctrine on I&W against non-cyber threats and interviews with cybersecurity experts, we propose the following general definition for cyber I&W frameworks and approaches:

> *An analytical process focused on collecting and analyzing information from a broad array of sources to develop indicators which can facilitate the prediction, early detection, and warning of cyber incidents relative to one's information environment.*

When discussing the scope and purpose of I&W frameworks in the cyber domain in

more detail, however, representatives from the private sector, NATO agencies, and the U.S. government define the concept differently. Some experts contend that I&W in cyberspace is primarily focused on gathering technical information on impending cyber threats, while others consider the concept to also include a survey of geopolitical developments that can influence a decision to initiate a cyber incident. Expert opinion also differs regarding the temporal parameters of the term. Some indicate cyber I&W frameworks should encompass monitoring the entire spectrum of cyberattack stages as outlined by Lockheed Martin's Kill Chain, to include detection of cyber incidents after the delivery stage.[3] Other cybersecurity experts see the utility of I&W frameworks as primarily focused on predicting incidents before they reach the delivery stage and while they are still in the reconnaissance stage, and even beforehand (INSA 2018, 3; Correspondence with cybersecurity experts and a NATO representative, December 4-21, 2018).

The U.S. Department of Defense's doctrine for cyberspace operations, DoD Joint Publication 3-12, provides useful clarity on the data-collection methods and techniques that warning intelligence applied to the cyber domain should include, and on the specific nature of cyber threats. The document stipulates that "cyberspace threat intelligence includes all-source analysis to factor in political, military, and technical warning intelligence. Adversary cyberspace actions may occur separate from, and well in advance of, related activities in the physical domains. Additionally, cyberspace threat sensors may recognize malicious activity with only a very short time available to respond. These factors make the inclusion of all-source intelligence analysis very important for effectively assessing adversaries' intentions in cyberspace." (Department of Defense 2018, IV-7) Yet, JP 3-12 and other U.S. doctrinal documents have not yet provided clear definitions and guidelines about how warning methodologies for cyber threats should be developed and how they should be incorporated in existing warning frameworks. Furthermore, existing U.S. documents fail to provide guidance for acceptable courses of action or responses given impending cyber threats.

3. CLASSIC I&W FRAMEWORKS

There are several well-known and widely-used I&W frameworks that the U.S. IC has been using to monitor and detect potentially threatening adversary behavior. Two such classic frameworks, summarized in this section, are the Lockwood Analytical Method for Prediction (LAMP) and the DoD's *Defense Warning Network Handbook* (Lockwood 2002, Joint Chiefs of Staff). These approaches can serve as the foundation in formulating a cyber I&W framework.

3 The seven-step Lockheed Martin Kill Chain is a well-known framework for mapping the stages of cyber incidents in support of intelligence-driven defense. For more information, see Muckin and Fitch, 2019.

I&W entails a probabilistic analysis, in which an analyst attempts to provide an assessment which is as realistic and objective as possible, given data and time constraints. A knowledge of history, doctrine, and precedent is critical in this process (Goldman 2002, 13). Specifically, when compiling indicator lists, analysts draw primarily from three sources: logic or longtime historical precedent, lessons learned from the behavior of threat actors during a recent war or crisis, and specific knowledge of the military doctrine or practices of the threat actors (Goldman 2002, 26).[4] One of the seminal warning intelligence analysts, Cynthia Grabo, argued that a robust warning methodology should incorporate both military and political indicators, prioritize indicators, and examine a variety of data sources in context (Grabo 1987).

The LAMP is one such framework that applies structure to the warning intelligence problem (Lockwood 2002). It assumes that the future is a spectrum of changing relative probabilities and aims to determine the relative probability of alternative futures. It consists of the following 12 steps:

1. Define the intelligence question under consideration with sufficient specificity and narrowness of enquiry
2. Specify the actors involved in the problem
3. Study each actor's intentions and perceptions of the problem
4. Specify all possible courses of action for each actor
5. Determine the major scenarios
6. Calculate the total number of alternate futures
7. Perform a pairwise comparison of all alternate futures within each scenario to establish their relative probabilities
8. Rank the alternate futures for each scenario from highest relative probability to lowest relative probability
9. For each alternative future, analyze the scenario in terms of its consequences for the intelligence question
10. Determine focal events that must happen to realize each future
11. Develop indicators for each focal event
12. State the potential of a given alternate future to transpose into another alternate future (Lockwood 2002, 2010; Singh 2013).

LAMP provides significant leeway for defining the number of major scenarios and the breadth of problems with which one is concerned. Although it does not define the exact form of comparison (e.g., Delphi method, survey, Bayesian inference) to use when developing the relative rankings of alternative future scenarios, the framework clearly relies on the talents of the individuals engaged in the process and therefore could result in different outcomes. That said, it is amenable to evaluation and adjustment

4 In this context, logic is tied to an actor's historical pattern of behavior - rather than based on an actor-agnostic theory, such as rational choice theory.

over time as events do (or do not) come to pass, providing a means to "grade" the probabilities.

The DoD's *Defense Warning Network Handbook* provides a similar set of steps as LAMP, but without the assignment of probabilities:

1) Identify anomalies/imagine alternatives
2) Produce scenarios
3) Identify conditions, drivers, and indicators
4) Determine warning threshold
5) Explore opportunities to influence or mitigate the threat
6) Communicate warning (Joint Chiefs of Staff).

As with LAMP, the DoD approach depends on the talents and experience of those engaged in the process. The U.S. IC has changed its intelligence approach over time, including having dedicated offices and analysts focused on warning, relative to other periods when warning was one of several duties assigned to analytic offices (Gentry and Gordon 2018). The two general warning frameworks provided here share a common approach that relies on speculating on potential futures which would be of concern, and crafting indicators which would provide early pointers towards that future coming to pass. These approaches rely on others within the military, intelligence, and defense communities to take action based on these warnings. Both frameworks offer a systematic way to monitor and detect threats and contain valuable components that can inform a cyber I&W framework; but are not sufficiently detailed to provide practical guidance for practitioners.

4. I&W FRAMEWORKS FOR CYBER THREATS

Experts have conducted promising initial research into adapting classic I&W frameworks or key components of the intelligence I&W cycle to the cyber domain. It is worth reviewing some of this research to demonstrate its applicability and build upon its strengths.

General I&W frameworks vary from cyber-specific frameworks in several areas, including in terms of the target of the analysis (i.e. physical/conventional/kinetic threats vs. cyber threats), but the classic frameworks can be adapted to address cyber threats. Another consideration is the partial divergence in analytical approaches. Specifically, classic intelligence analysis is primarily backward-looking and forensically focused, while cyber I&W framework may incorporate predictive analytical techniques that add a forward-focused analytical component. Nevertheless, the classic frameworks can

inform the design of a robust I&W methodology for cyber incidents, while analytical processes, data-collection techniques, and methodologies can also be transferable across the two frameworks.

One such approach is a twelve-step adaptation of Lockwood's LAMP method by Robinson et al (2012):

1. Problem identification: determine the issue
2. Identify potential actors
3. Actor courses of action: viability and probability (include the Kill Chain here)
4. Determine scenario enablement
5. Manifested scenario focal events
6. Create focal event indicators: an adversary prepares for hostilities
7. Collect and monitor through indicators: assess emerging trends
8. Discern the probable scenario that is trending
9. Readjust for new manifestations of the scenario
10. Deception in indicators
11. Mental model avoidance: is it expectation or actuality, theory or current developments?
12. Strategic options analyzed against viable scenarios (Robinson, Astrich and Swanson, 2012).

More recently, the Intelligence and National Security Alliance (INSA) published a working group report that proposes a high-level conceptual framework against cyber threats, consisting of the following seven steps:[5]

1. Identify & prioritize assets – identify which data, devices, personnel, and facilities are most critical to the organization
2. Refine the threat – identify which top 10 or 15 cyber threats may inflict the most damage to the assets listed in step 1
3. Assess threat courses of action – design adversaries' Course of Action (COA) based on scenarios; can use the Lockheed Martin's Kill Chain or MITRE's ATT&CK methodology
4. Break down scenarios into IOCs
5. Plan and exercise countermeasures
6. Align to the intelligence cycle
7. Execute proactive countermeasures (INSA 2018, 12-7).

The valuable contribution from the INSA approach is to combine the outward focus of warning frameworks (i.e., what scenarios we are concerned about) with an inward

5 INSA is a U.S.-based nonprofit organization founded in 1979 that provides a platform for the development and promotion of public-private solutions to national security challenges. For more information, see https://www.insaonline.org/about/.

focus on what those scenarios would impact. It begins by identifying and prioritizing the assets which an organization should seek to protect, and proceeds by understanding various threat actors' courses of action.[6]

5. COMPARISON OF EXISTING I&W FRAMEWORKS

Each of the four frameworks discussed provides insights into developing indications and warning for cyber threats. The two traditional intelligence processes, developed by the Defense Intelligence Agency and Lockwood, are general approaches which should be applied and made more specific to the cyber domain, but do provide a structured and logical approach. Robinson has attempted to do that with Lockwood's approach; while the INSA paper provides a different view on applying traditional intelligence community approaches. Below, we have mapped these four frameworks against general categories of analysis and action to highlight where they overlap and combine their elements into a synthesized approach.

Although not high-level cyber I&W frameworks, there are two other important approaches used to understand how malicious actors plan and conduct cyberattacks: Lockheed Martin's Cyber Kill Chain and MITRE's Adversary Tactics, Techniques, and Common Knowledge (ATT&CK). Both approaches start with the premise that understanding the steps a malicious cyber actor must accomplish to plan and execute an operation can help a cyber defender understand what activity to look for and the defensive measures to implement. The Kill Chain consists of seven steps: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives (Lockheed Martin 2015).

The ATT&CK framework was developed to provide a common taxonomy for mapping real-world observed behavior and techniques. It maps a technique to a stage of an operation and provides insight into what that technique is supposed to accomplish. Cyber Red Teams can use the framework to develop playbooks based on real-world experience, as well as show what techniques or exploits are most commonly used by Advanced Persistent Threats (APTs).[7] The framework, similar to the Cyber Kill Chain but with additional depth, maps techniques to the stages of an intrusion. In

6 MITRE has developed a method for identifying critical cyber assets called Crown Jewel Analysis. Similar to mission assurance analysis, it starts with identification of critical missions and the assets those missions rely upon. See the MITRE Corporation. For more on this approach, see https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

7 For a general overview of the origins and use of the ATT&CK framework, see Strom, 2018. Playbook is a term used to describe a specific sequential collection of ATT&CK framework-mapped post-exploitation techniques employed by an adversary as they move through the Kill Chain phases of Installation, Command & Control and Actions on Objectives, under which MITRE's ATT&CK framework's 11 tactics logically fall. Each playbook is essentially a post-exploitation threat model, understanding that an adversary may use the same playbook for each operation or change technique combinations over time.

the case of ATT&CK, it has eleven stages tied to the desired objective for the stage: initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration, and command and control.[8] More recently, MITRE has been developing a PRE-ATT&CK model to try to identify the stages of cyberattack planning prior to access to a network.

There are several insights to draw from this mapping. The frameworks vary in terms of the level of specificity they provide for a given step. The Lockwood approach, for example, provides several steps for developing scenarios, but Robinson's adaptation of Lockwood captures these in fewer steps. The DIA framework focuses ultimately on communicating warning (which we have placed in a general category of "acting" on indicators). While being less specific on recommending steps for generating scenarios, the DoD framework emphasizes the policy relevance of an I&W approach, while Lockwood does not address either tracking or acting. In comparison to the others, Robinson's framework is more focused on tracking, adjusting and acting on the indicators.

All frameworks contain valuable elements for a cyber I&W framework, but no one approach appears to incorporate the classic lessons of effective threat intelligence which Grabo, among others, advocated: such as conducting both technical and strategic assessment of threat actors and their environment, as well as clearly emphasizing the need to produce actionable information useful for policymakers. Therefore, the frameworks can be consolidated to inform the design of a cyber I&W approach that comprehensively addresses these issues and can be applied to the structure of an organization to inform decision-making.

6. RAND'S PRACTICAL APPROACH FOR CYBER I&W

RAND proposes the following approach for cyber I&W, which offers a practical, hands-on workflow for cyber defenders; synthesizes and adds onto many of the components of the other I&W frameworks; and would typically belong in an organization's Cyber Threat Intelligence (CTI) program. The steps of RAND's approach all take place in the first phase of cyber incident response: preparation (Kral 2011).[9] The approach explicitly accounts for both technical assessments (e.g., what are the most commonly used playbooks of APT actors that are likely to target a network?) and contextual, geopolitical assessments (e.g., what military, political, economic or social developments influence a decision to initiate an incident?) to understand the broader operating environment. Adding a focus on the strategic environment moves beyond the technical aspects of cybersecurity to attempt to understand the external factors that

8 The full framework can be found at https://attack.mitre.org.

9 The phases of incident response are as follows: preparation, identification, containment, eradication, recovery and lessons learned. Only the first phase, preparation, aligns with the predictive and anticipatory nature of I&W. See Kral 2011.

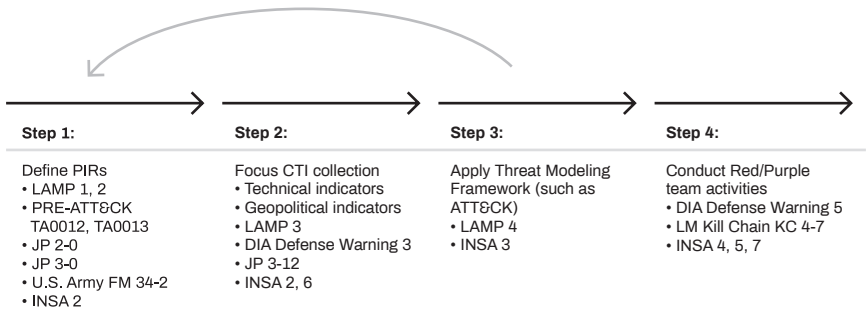
TABLE 1: A COMPARISON OF CLASSIC AND CYBER INDICATION AND WARNING FRAMEWORKS

General Actions	Classic I&W Frameworks		Cyber I&W Frameworks	
	Defense Warning Handbook	LAMP / Lockwood	Robinson (adopted from LAMP)	INSA
Framing Questions		1.Define the intelligence question under consideration with sufficient specificity and narrowness of enquiry	1. Problem identification: determine the issue	
Identify Threats		2. Specify the actors involved in the problem 3. Study each actor's intentions and perceptions of the problem 4. Specify all possible courses of action for each actor	2. Identify potential actors 3. Actor courses of action: viability and probability (include the Kill Chain here)	2. Develop a refined understanding of the most likely threats
Identify Assets to Defend				1. Identify and prioritize assets to be protected
Develop Scenarios	1) Identify anomalies/imagine alternatives 2) Produce scenarios	5. Determine the major scenarios 6. Calculate the total number of alternate futures 7. Perform a pairwise comparison of all alternate futures within each scenario to establish their relative probabilities 8. Rank the alternate futures for each scenario from highest relative probability to lowest relative probability 9. For each alternate future, analyze the scenario in terms of its consequences for the intelligence question	4. Determine scenario enablement 5. Manifested scenario focal events	3. Using structured analytic techniques, forecast likely attack scenarios
Develop Indicators	3) Identify conditions, drivers and indicators 4) Determine warning threshold	10. Determine focal events that must happen to realize each future 11. Develop indicators for each focal event 12. State the potential of a given alternate future to transpose into another alternate future	6. Create focal event indicators: an adversary prepares for hostilities	4. Decompose scenarios into indicators of likely adversary actions
Track Indicators	5) Explore opportunities to influence or mitigate the threat		7. Collect and monitor through indicators: assess emerging trends 8. Discern the probable scenario that is trending	6. Collect intelligence on indicators and adversary plans and intentions
Act on Indicators	6) Communicate warning		9. Readjust for new manifestations of the scenario 10. Deception in indicators 11. Mental model avoidance: is it expectation or actuality; theory or current development? 12. Strategic options analyzed against viable scenarios	5. Plan and exercise countermeasures to likely adversary actions 7. Execute proactive measures to counter anticipated attack vectors

indicate intent and timing behind adversary cyber activity. As such, corollary focused CTI collection combined with a strategic all-source approach may help answer "Why?" and "When?" questions, to give defenders further indications and warning as to the probability of a cyber incident.

RAND's Practical Approach for Cyber I&W begins with suggesting the use of Priority Intelligence Requirements (PIRs). This leads to an iterative loop with CTI collection, then to employment of systematically-constructed playbooks of adversarial techniques and behavior, by leveraging a threat modeling framework such as MITRE's ATT&CK. Finally, Red/Purple Team activities emulate relevant threats, check for visibility gaps, and allow mitigations to be designed.[10] This approach should be accessible and usable to cyber defense teams at all levels of capability maturity. Figure 1 shows our approach, followed by a high-level overview of each of the steps. Depending on an organization's resources and capabilities, much more depth can exist within each step as an organization's resources and capabilities allow.

FIGURE 1. RAND'S PRACTICAL APPROACH FOR CYBER I&W

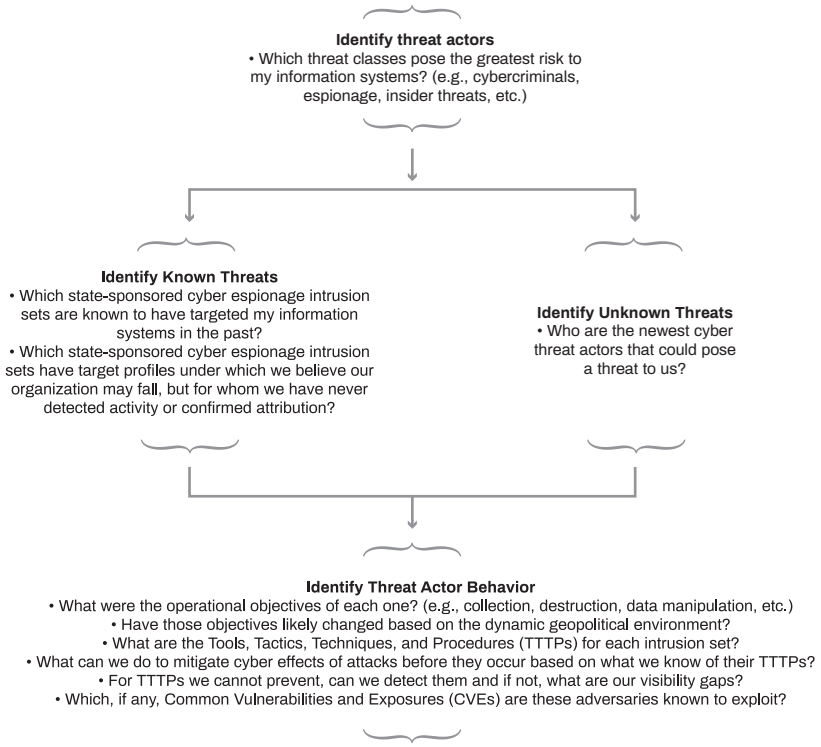


Step 1: Define PIRs

Anticipation of threats can be facilitated by a simplified approach of developing some basic PIRs from a cyber defense perspective. PIRs consist of a concise set of questions devised, prioritized, regularly updated, and continuously answered to better understand one's adversaries by allowing the defenders to focus their CTI collection. Examples of PIRs developed to facilitate discovery of I&W for cyber incidents within a cyber defense operation's CTI Program are shown in Figure 2.

10 A Purple Team (red + blue) is a modification of a traditional Red Team, where the offensive cyber operations (Red Team operations) are conducted side by side with or by cyber defense analysts (Blue Team operations) against one's own network. This can have numerous benefits. Purple Teams work well in many organizations but not all; some still benefit from the hard separation, in which case an organization may choose to substitute our usage of Purple Teams with the traditional Red Team approach.

FIGURE 2: EXAMPLE PIRS TO FACILITATE DISCOVERY OF CYBER I&W



Relative to other frameworks reviewed in this article, PIRs relate closely to LAMP steps 1 and 2, as well as the first two tactics described by MITRE's PRE-ATT&CK framework: priority definition planning (TA0012) and priority definition direction (TA0013). It also maps to what INSA's Framework for Cyber I&W lists as step 2.

Step 2: Use the Derived PIRs to Focus CTI Collection

CTI can often answer "Who?", "What?", "Where?" and "How?" questions, helping to understand adversaries' behaviors and tools, tactics, techniques, and procedures (TTTPs), thus strengthening I&W and cyber incident preparation or prevention. The findings from RAND's step 1 help drive CTI collection requirements and filter the mountain of tactical-level IOCs (e.g., malicious IP addresses, domains or hashes) that correspond to intrusion sets other than those targeting the organization, and strategic-level geopolitical developments (e.g., incoming national elections or recalling reservists) that could be indicative of probable adversary action to help scope and focus collection to what matters most to the organization, given the reality of limited resources.

Harnessing CTI in this way closely relates to LAMP step 3, DIA's Defense Warning Handbook step 3, and INSA's steps 2 and 6, and can also incorporate all-source intelligence collection for additional strategic context, to better help answer "When?" or "Why?" questions that may be defined in PIRs (see JP 3-12). Relevant CTI uncovered in response to PIRs such as, "Which, if any, CVEs are these adversaries known to exploit?" can also serve as vulnerability exploitation intelligence, informing enterprise patching prioritization efforts. Automated operationalization of IOCs from CTI is recommended - but describing this process is beyond the scope of this article.

Step 3: Apply Adversary Threat Modeling Framework: MITRE's ATT&CK

Step 3 of the approach is analogous to a narrowed LAMP step 4 and INSA's step 3. It takes the findings of which intrusion sets are targeting one's organization and enters them into an adversary threat modeling framework, such as MITRE's Enterprise ATT&CK Navigator (an interactive JavaScript-based version of the framework).[11] This helps prioritize an organization's focus on pre-mitigating probable attacks by being able to prevent or detect the specific techniques employed by one's adversaries. Once the most relevant TTTPs are identified, cyber defenders can use the information as inputs to a Red Team statement of work or Purple Team task list. MITRE's PRE-ATT&CK and ATT&CK framework has expanded upon Lockheed Martin's cyber intrusion Kill Chain, to originally include treating Kill Chain steps as akin to overarching tactics (represented as column heads) under which many techniques fall.

Step 4: Conduct Continuous Red / Purple Team Ops

The final step in RAND's Practical Approach for Cyber I&W is the culmination of all previous steps: it tests relevant adversary TTTPs and playbooks against the organization's environment. By this stage, the defenders know who their threats are, how they behave, the details of their tools (capability/how), when (opportunity), and why (intent) they might attack. In this step, if using the Purple Team concept, the defender emulates adversary behavior and current playbooks as closely as possible while tuning defenses to prepare for a potential similar incident. Performing these activities is akin to step 5 of the DIA Warning framework, and incorporates steps 4, 5, and 7 of the INSA framework. Another advantage this step has is that it allows cyber defenders to continuously discover, understand and test for detection visibility gaps, continuously improve their Security Information and Event Management (SIEM) and other detection content, and improve the security settings or architectural design details of an organization's network ahead of time. It also allows an organization to define and refine Courses of Action (COAs) to take during the containment phase of an attack, each of which can map to different phases of the Lockheed Martin cyber intrusion Kill Chain.

11 https://mitre-attack.github.io/attack-navigator/enterprise/

7. CASE STUDY – NOVEMBER 14, 2018 APT29 SPEAR-PHISHING CAMPAIGN

Finally, we share a real-world example of an organization applying the RAND practical approach to the cyber I&W set forth in this article: integrated into normal cyber defense operations against the backdrop of strategic geopolitics, corresponding cyber espionage activity, and "friendly" government agencies conducting their own cyber I&W and counter-threat operations. The example involves the widespread November 14, 2018 post-midterm U.S. election phishing campaign, widely believed to have been perpetrated by the Russian-nexus intrusion set publicly known as APT29 (attributed to the Russian Foreign Intelligence Service (SVR), see Modderkolk 2018). We use "Organization Z" to denote one of the targets of the November attack, and describe examples of their cyber I&W actions to prepare for a probable attack.

Application of the cyber I&W process in this case resulted in Organization Z predicting and assessing with moderate confidence that APT29 would attempt a cyber intrusion against it, corresponding to the U.S. midterm elections, based on past adversary patterns. As some APT intrusion sets have shifted to or experimented with more generic or commodity malware or tools in an attempt to further obscure their origins for the purpose of making attribution more difficult, Organization Z had applied all steps of this approach not only to APT29's TTTPs, but also to tools more commonly used not just by legitimate Red Team operators, but some APT groups too. Organization Z's widening of scope for what tool to test for a Purple Team task is an example of efficiency when selecting a tool or technique from the ATT&CK framework in RAND's step 3 to test in RAND's step 4.

The tool selected in step 3 was based on answering step 1 PIRs: "Which state-sponsored cyber espionage intrusion sets are known to have targeted my information systems in the past?"; and "What are the TTTPs for each intrusion set?" The answers to these two PIRs resulted in the decision to focus Organization Z's specific CTI collection requirements in step 2. Multiple APT groups as well as Red Team operators use commodity tools. This is illustrative of an advantage that can be taken back by defenders in an analog of attacker/defender co-evolutionary adaptation, giving rise to increased cyber resiliency despite changing adversary tools and predictability.

This preparation resulted in Organization Z using threat emulation software, Cobalt Strike, on its network during internal Purple Team activities in preparation for a variety of threats.[12] This led to improved SIEM content, verification of detection and

12 Cobalt Strike is a commercial, full-featured, penetration testing tool which bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors." Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system. (https://cobaltstrike.com/downloads/csmanual38.pdf)

prevention capabilities, tool integration and automation.[13] During this test, detection of the type of beacon was confirmed, integration of security platforms demonstrated value, and SIEM content was created to notify Organization Z's cyber defense team via email if the selected events deemed critical occurred.

Just weeks after conclusion of the testing, and the day before election day and the expected intrusion attempt, on November 5, 2018, USCYBERCOM announced that "the Cyber National Mission Force, a unit subordinate to U.S. Cyber Command, posted its first malware sample to the website VirusTotal…"[14] The initial focus of uploads was unclassified malware samples attributed to Russia. The timing of this did not seem coincidental and appeared suggestive of a larger plan aimed to disrupt any potential Russian interference in the midterm elections, which was suspected based on Russia's interference in the 2016 U.S. presidential elections. November 6, 2018 (election day) passed without incident. Did USCYBERCOM, with all their resources, have their own cyber I&W that APT29 was going to perpetrate a large attack? Was the November 5, 2018 change in policy - uploading voluminous malware samples associated with Russian espionage - part of an attempt to disrupt the attack?

Eight days after the election, on November 14, the APT29's offensive cyber operation was finally conducted, but the initial tool used during the exploitation phase of the Kill Chain was a Cobalt Strike Beacon payload, with a modified Pandora malleable Command and Control (C2) (Dunwoody et al., 2018). It was previously unseen as a tool used by this intrusion set and is a widely available commodity tool, with the Pandora malleable C2 available as open-source code on GitHub. There are unanswered "Why?" questions in this case, but ultimately the intrusion attempt against Organization Z was unsuccessful and quickly contained.

USCYBERCOM was unable to stop this attack from happening entirely, but one of Organization Z's hypotheses as to why the attack was delayed by eight days was that USCYBERCOM disrupted the attack initially on or before November 6. It is possible that the uploaded malware samples or something else resulted in a change in tools by the adversary. The C2 domain was registered on October 15, 2018, yet it could have initially been intended for communication with another tool, beacon or malware specimen.[15]

13 These details illustrate the tip of the iceberg on how an organization can go as deep as they have the resources for - chiefly based on their time and personnel availability - but additional expansion was beyond the scope of this article.

14 "…Recognizing the value of collaboration with the public sector, the Cyber National Mission Force (CNMF) has initiated an effort to share unclassified malware samples it has discovered that it believes will have the greatest impact on improving global cybersecurity. For members of the security community, CNMF-discovered malware samples will be logged at this website: https://www.virustotal.com/en/user/CYBERCOM_Malware_Alert/".

15 One can check domain registration dates and history by querying domain registration or passive DNS records.

As was revealed in late February 2019, there was a larger plan by USCYBERCOM, approved by the President and Congress and coordinated among numerous government agencies, to protect against election interference with an offensive cyber campaign. The authority was afforded by National Security Presidential Memorandum 13 (Nakashima 2018). The malware which USCYBERCOM uploaded to VirusTotal and the announcement about it seem to have formed only one small piece of a larger strategy that the public was able to glimpse at the time; and even though the specific malware uploaded was not likely to have involved new adversary tools, perhaps it had a psychological effect that affected adversary behavior and planning.

From an I&W perspective, this particular case study underscores the challenge of predictive analysis when many variables are at play, and also illustrates the interconnected and dynamic reality of the operating environment when other friendly agencies take calculated actions that possibly affect adversary behavior and disrupt some basic predictability which another organization may have established. It also highlights the potential increased resiliency that RAND's proposed practical cyber I&W approach can bring about. Perhaps resilience is more important than knowing precisely when and how an attack will occur, though a combination of the two would constitute the best case scenario from a defender's perspective.

8. CONCLUSION

Much can be learned from an examination of traditional strategic I&W intelligence frameworks, as well as the main methodological and analytical challenges that the I&W field has faced and already addressed, though significant differences in the cyber domain do exist when it comes to applying a practical workflow to operationalize collected intelligence. Despite these differences, however, both the cyber domain and traditional strategic I&W frameworks applied to the four other domains use overlapping methods and techniques for threat modeling and intelligence collection and exploitation, which can serve as a methodologically sound foundation for steps constituting a newly codified approach of addressing anticipated cyber threats.

RAND's proposed Practical Approach for Cyber I&W consists of four steps; each corresponds to and draws upon previously reviewed I&W frameworks. This overall approach accounts for collection, processing, and operationalization of filtered tactical, operational and strategic CTI, to determine and understand relevant adversaries within the context of the broader geopolitical environment as it relates to the network being defended. It also leverages MITRE's ATT&CK as an example of applying a threat modeling framework and to some extent, the PRE-ATT&CK extension.

An organization taking this approach to cyber I&W, integrating it into their cyber defense operations, and adding their own creativity and toolsets to expand, refine, and tailor the processes within each step can continuously improve readiness, prioritize limited resources, and enhance overall resilience to cyber incidents. This approach is also intended to be accessible by any cyber defense team at any capability maturity level; and as an organization's capabilities increase, they can iterate, automate, and expand processes in each step as they wish. For example, incorporating even more ideas from traditional I&W frameworks to develop new PIRs or improve COAs is easy to add to steps 1 or 4 respectively.

The November 14, 2018 spear-phishing campaign by Russia's APT29 against U.S. government agencies, think tanks, and businesses demonstrates how the proposed cyber I&W approach can be integrated into cyber defense operations and applied to achieve resiliency against cyber adversaries, despite inevitable unpredictability.

REFERENCES

Blackshaw, Amy. 2016. "Behavior Analytics: The Key to Rapid Detection and Response?" *RSA*. https://www.rsa.com/en-us/blog/2016-01/behavior-analytics-the-key-to-rapid-detection-response.

DeCianno, Jessica. 2014. "Indicators of Attack vs. Indicators of Compromise," *CrowdStrike*. December 9. https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/.

Defense Intelligence Agency. 2014. "Instruction 3000.001, Enclosure 1, 27 May". In Defense Intelligence Agency, "Warning Fundamentals", Unclassified briefing, 3.

Defense Intelligence Agency. "Warning Fundamentals." Unclassified briefing.

Department of Defense. 2013. "Joint Intelligence, Joint Publication 2-0." October 22. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf.

Department of Defense. 2018. "Cyberspace Operations. Joint Publication 3-12." June 8. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

Dunwoody, Matthew, Andrew Thompson, Ben Withnell, Jonathan Leathery, Michael Matonis, and Nick Carr. "Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign." *FireEye*. November 19, 2018. https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html.

Gentry, John and Joseph Gordon. 2018. "US Strategic Warning Intelligence: Situation and prospects." *International Journal of Intelligence and Counterintelligence* 31(1): 19-53.

Goldman, Jan (ed.). 2002. *Anticipating Surprise: Analysis for Strategic Warning*. Center for Strategic Intelligence Research: Joint Military Intelligence College.

Grabo, Cynthia. 1987. *Warning Intelligence*. The Intelligence Profession Series: Association of Former Intelligence Officers.

Hernandez-Suarez, Aldo, et al. 2018. "Social Sentiment Sensor in Twitter for Predicting Cyber-Attacks Using ℓ1 Regularization." *Sensors* 18(5): 1380.

Husák, M., et al. 2018. “Survey of Attack Projection, Prediction, and Forecasting in Cyber Security.” *IEEE Communications Surveys & Tutorials*: 1-21. https://ieeexplore.ieee.org/document/8470942/.

INSA. 2018. “A Framework for Cyber Indications and Warning”. *Intelligence and National Security Alliance*. October. https://www.insaonline.org/wp-content/uploads/2018/10/INSA-Framework-For-Cyber-Indications-and-Warning.pdf.

JMIC. 2001. “Warning Glossary.” This is not a publicly released document.

Joint Chiefs of Staff. 2017. “Joint Publication 3-0. Joint Operations. January 17, Incorporating Change 1, October 22, 2018.” http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

Joint Chiefs of Staff. “Joint Staff J2. Defense Warning Staff. J2 Warning.” *Defense Warning Network Handbook*. 4th ed. This is not a publicly released document.

Kral, Patrick. “The Incident Handler’s Handbook.” *SANS Institute InfoSec Reading Room*, February 21, 2012. https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

Lockheed Martin. 2015. “Gaining the Advantage: Applying Cyber Kill Chain ® Methodology to Network Defense 2015”. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

Lockwood, Jonathan. 2002. “The Lockwood Analytic Method for Prediction (LAMP). An Innovative Methodological Approach to the Problem of Predictive Analysis.” *LAMP-Method*. January. http://lamp-method.org/lampppt.ppt.

Lockwood, Jonathan. 2010. “The Application of LAMP.” http://lamp-method.org/2.html.

Modderkolk, Huib. 2018.“Dutch agencies provide crucial intel about Russia’s interference in US-elections.” *De Volkskrant*, January 25. https://www.volkskrant.nl/media/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/.

Muckin, Michael and Scott C. Fitch. 2019. “A Threat-Driven Approach to Cyber Security Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization,” *Lockheed Martin Corporation*. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf.

Nakashima, Ellen. “White House Authorizes ‘Offensive Cyber Operations’ to Deter Foreign Adversaries.” *The Washington Post*. September 20, 2018. Accessed March 09, 2019. https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?utm_term=.510d18f07e45.

Robb, Drew. 2017. “Eight Top Threat Intelligence Platforms.” *eSecurity Planet*. July 18. https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html.

Robinson, Michael, Craig Astrich and Scott Swanson. 2012. “Cyber Threat Indications & Warning: Predict, identify and counter.” *Small Wars Journal*. July 26.

Singh, Jai. 2013. “The Lockwood Analytical Method for Prediction within a Probabilistic Framework.” *Journal of Strategic Security* 6(3): 83-99.

Strom, Blake. 2018. “ATT&CK 101.” May 3. *The MITRE Corporation*. https://medium.com/mitre-attack/att-ck-101-17074d3bc62.

The MITRE Corporation, “Crown Jewels Analysis,” *MITRE Systems Engineering Guide*. https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

U.S. Code of Federal Regulations. “Title 48. Chapter 2. Subchapter H. Part 252. Subpart 252.2. Section 252.204-7012.”

U.S. Cyber Command. 2018. “New CNMF initiative shares malware samples with cybersecurity industry.” November 5. https://www.cybercom.mil/Media/News/News-Display/Article/1681533/new-cnmf-initiative-shares-malware-samples-with-cybersecurity-industry/

Watson, Bruce, Susan Watson and Gerald Hopple. 1990. “United States Intelligence: An Encyclopedia”. New York: Garland Publishing, Inc., 594. In *JMIC Warning Glossary 2001*.