Cyber Threat Intelligence (CTI) Team Intelligence Requirements

We intend to assist cyber threat intelligence teams in the development of proper intelligence requirements. The following outlines measures needed to effectively define intelligence requirements, determine nation-state and adversary/threat actor intent and capabilities, reviewing corporate 'crown jewel' information provided by other groups, combined with pertinent taxonomy and sample matrices. We hope this assists in your efforts to mature your intelligence program.

Prioritization

The effective management of your intelligence activities relies on prioritizing the intelligence requirements against *available intelligence capabilities*. For this reason, we write intelligence requirements and prioritize them determined by the ability of the resulting intelligence to inform the stakeholders and support their decisions.

The relative assigned priority of an intelligence requirement reflects the criticality of the decision it supports. Simply put, some decisions are more critical than others. For instance, identifying a new threat actor without a clear understanding of the actor's capabilities is less of a priority than an existing threat actor known to your organization with new infiltration methods and a change in espionage intent sabotage in the form of disk wiping.

> Of note: intelligence collection, analysis, and reporting should focus on critical systems and data. Standard intelligence requirements do not include publicly communicated software vulnerabilities or control weaknesses in a desktop office suite. Consider weaknesses a risk due to the vulnerability that requires modification(s) to process or technology controls such as stop gaps before a patch. These are functions of risk, vulnerability management, and day-to-day security operations, better known as routine information security hygiene.

The intelligence effort needed to drive your CTI team findings and high-level recommendations should follow suit. The intelligence function receives prioritized data on critical systems, sensitive information (personally identifiable information, intellectual property, etc.), supply chain organizations (internal/external – hardware/software), and other areas of concern for the corporation. The combination of the above with stated requirements from stakeholders are factors in prioritization. The intelligence organization is not charged with gathering and maintaining critical systems and sensitive information but uses that knowledge to craft intelligence requirements.

A thorough understanding of the stakeholder's intent, knowledge of the supported plan, and anticipated decisions included therein should guide PIR nominations for approval.

Narrowly defined intelligence requirements help the prioritization process.

> Due to the many topics they address, broadly posed questions are challenging to answer and difficult to parse.
>
> Difficulties associated with dividing an intelligence requirement into its parts makes it difficult to prioritize the entirety of the collection and production workload associated with them.
>
> Because of their scope, broadly crafted questions often include low priority topics.

2018 Treadstone 71 LLC

Intelligence collectors should routinely collaborate with analysts to identify what intelligence is already known and what intelligence is not known. Jointly, collectors and analysts assess the production of new information and intelligence to inform decisions during planning or to guide operations. *The iterative process occurs automatically and focuses on the gaps in knowledge, analysis, and collection.*

Ideally, each of the supporting production requirements entered should prescribe only one verb (i.e., the analytic task to be performed) and one object to be analyzed.

Intelligence requirements do generally not focus on indicators of compromise, patch management, desktop software, smartphones, or other like-devices.

- *Intelligence requirements drive collection.*
- *The collection maintains data provenance.*
- *Data analysis drives reporting and briefing.*
- *Analytic reports forecast and warn.*

Preferably, we should pose questions in a manner that their answers create a decision "advantage." That is, craft questions to allow stakeholders direct action before it is too late. The continuous gathering of information within the context of the strategic end state and assessment processes allows CTI Team to keep their respective running staff estimates. By collecting and analyzing information about changes to the operational environment, changes to system behavior, or changes to adversary capabilities, analysts can draw conclusions related to the next series of adversary courses of action (CoA) and provide early warning.

Intelligence analysts must understand all relevant aspects of the operating environment. Our situational understanding should include the adversary's disposition and the socio-cultural nuances of individuals and groups in the operating environment. Stakeholders require and expect timely intelligence estimates that accurately identify adversary intentions, support information security and associated groups adjustments to controls, threat levels, and security posture, and estimate future adversary CoA in sufficient detail to be actionable.

Distill this mass of information into intelligence to support an estimate of the situation and adversary capabilities and intentions. The estimative nature of intelligence distinguishes it from the mass of other information available to stakeholders, including communicated vulnerabilities and available patches.

Intelligence should increase stakeholders understanding of the threat and adversary's probable intentions, end states, objectives, most likely and most dangerous CoA, strengths, and critical capabilities.

The overall question we are trying to answer is:

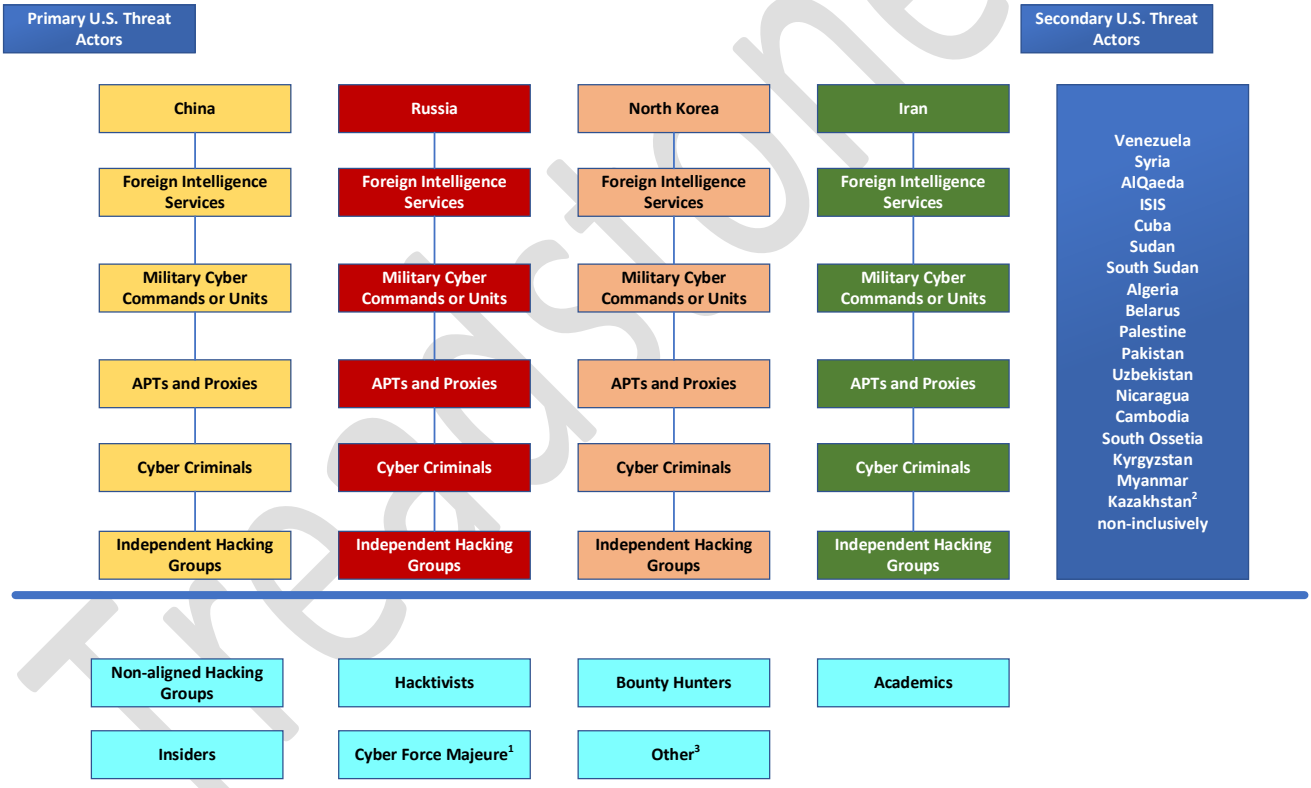
- Who would have the capabilities, patience, skill, sophistication, and resources necessary to execute a successful attack against our perimeter / critical organizational assets/hardware and software supply chains? The above is not an intelligence requirement but a general statement for decomposition and analysis.

Basic intelligence research further clarifies this question and provides the knowledge necessary to define intelligence requirements clearly. Until such time, the logical targets are those referenced in Figure 1 below and Figure 2 on the following page. Expand Current intelligence requirements on the targets (Figure 2) until the IRs are exhausted and the CTI Team receives the 'crown jewel' information.

2018 Treadstone 71 LLC

We recommend that the CTI Team perform a baseline intelligence study providing an information base against discovering, validating, monitoring, and assessing the main threat actors (human and otherwise). A logical series of actors aligned with national interests and known threat actors targeting the organization. The basic intelligence study is a research effort to validate and revalidate threat actors while tracking the organization's attack surface's progress and effectiveness. The research results in an intelligence assessment that details the threat, capabilities, and intentions of adversaries. Other questions and the associated data from the answers to those questions (See Section **Information Required Before Determining Intelligence Requirements** below) must be in place for an accurate understanding of the operational environment and intelligence requirements created.

The research combined with stakeholder needs to establish the backdrop for intelligence requirements (IRs) and the ability to shift to priority intelligence requirements (PIRs) when needed. This method



[1]Force majeure is generally intended to include occurrences beyond the reasonable control of a party, and therefore would not cover: Any result of the negligence or malfeasance of a party, which has a materially adverse effect on the ability of such party to perform its obligations. Any result of the usual and natural consequences of external forces. Any type of power, internet, or other such outage.
[2] The Top Tens - https://www.thetoptens.com/enemy-countries-groups-united-states/
[3] Other may include any new or existing threat not yet categorized

Figure 1 Logical Primary Targets

Treadstone 71

Adversary Country-Group-Capability-Intent Threat Matrix

ADVERSARY Country	North Korea	North Korea	Iran	China	Russia
Group-->	Lazarus Group, Appleworm, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY,Vedalia	APT10 (menuPass, Stone Panda, Red Apollo, CVNX, HOGFISH)	APT34 (Crambus/Chafer/Cadelle, OilRig, Helix Kitten)	APT1 (Comment Crew, Comment Group, Comment Panda, HiddenLynx)	APT28 (Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Swallowtail, Tsar Team, Threat Group-4127, TG-4127)
Intent	Espionage	Espionage	Espionage	Espionage	Espionage
Capability	Level 6	Level 5	Level 4	Level 5	Level 6
Potential Impact	High	High	Medium	High	High

Figure 2 Top 5 per the most recent RFI

supports situational awareness contributes to the intelligence preparation of the cyber battlefield and allows rapid shifts in priorities. The method also ensures changes from a strategic level (geopolitical/socio-cultural) through operational and tactical levels. During the study, a critical factor determines what indicators at the strategic, operational, and tactical levels to monitor. The study should deliver the minimum information needed to define the threat actors, their capabilities, intent, etc. (Figure 3 below). The study relates to the definition of indicators at any level:

- Observable / Collectible / Practical - An indicator can be observed and collected at suitable periods.
- Valid - An indicator must accurately measure the concept. The target's complexity drives the need for multiple indicators, but the objective is for the fewest possible.
- Reliable - Data collection must be consistent using comparable methods. People who are collecting must observe the same thing. Every indicator requires a precise definition.
- Stable - An indicator must be useful over time to allow comparisons and to track trends.
- Unique - An indicator should measure only one thing and only point to the studied activity in combination with the others.

Motive Intent Conditions	Who in the environment is advocating a change, wrong, grievance, etc.?
	What is the actor's capacity to act: is he charismatic, are others attracted to his message, can he organize a group, is there political power backing the actor, spouting propaganda, using influence operations to drive a point / create a wedge, etc.? What is driving the actor's motives? What is the intent of the actor when targeting the organization?
	What is the potential energy between the actor's motives and the conditions to take action?
	What is the condition moving the actor or group (centers of gravity), (e.g., anger, boredom, promoting a cause, nationalistic fervor, personal gain, monitization, disgruntlement, power/revenge, greed, ideology, espionage, sabotage, terrorism, religious beliefs, economic pressures, changes in the political environmental environment)?
Opportunity	What are the activities in the environment that provide the actor with the opportunity to take action (e.g., vulnerabilities, inclusion in social media sites, data dump, data exfiltration, social engineering, memetic engineering…)
Triggers	Is there a concentration of triggers that are moving the actor to take action? Are there geo-political, economic, or socio-cultural events that may drive cyber activity?
	Are these triggers being revealed and gaining in momentum (e.g., increased social media presence, online call to action, cyber protests, flooding social media with negative comments, fake stores claiming nation-state actions against their country or cause, ...)?
Course(s) of Action (Trajectory)	What is the actor's anticipated non-normative behavior and how can his CoA be changed? What are the normal TTPs related to this actor or group? Are there patterns and trends in timelines and chronologies related to this actor/group? What tendencies have been developed?
Capabilities	What are the cyber capabilities, expertise, levels of automation, maliciousness (i.e., destroy, disrupt, distort, disclose, discover)?

Figure 3 Non-inclusive areas minimum information – Naval Postgraduate School Paper

2018 Treadstone 71 LLC

Information Required Before Determining Intelligence Requirements (Crown Jewel information)

Certain information must be available for analysis before creating intelligence requirements. Define a clear area of concern providing accurate and timely intelligence requirements. The IRs include organizational assets of importance and trusted vendor/partner assets directly related to the organization.

The information required is the answers to the following questions. The information includes data from other internal organizations, research already performed, researched to be performed, including open-source collection:

- What data do we create and maintain that is of importance to the company? What laws protect that data?
- Where is that data located? How would we be impacted if it was discovered, distorted, disrupted, destroyed?
- What data do we obtain from clients that are of importance to the company? What laws protect that data?
- Where is that data located? ? How would we be impacted if discovered, distorted, disrupted, or destroyed?
- What products created, delivered, and supported by our suppliers are the most critical to the company's success?
- Where are they created, and by whom? What companies create what components that make up each of the critical products? Where is the IP around those products stored?
- What software created, delivered, and supported by us and our suppliers are the most critical to the success of the company
- What software created, delivered, and supported by us and our suppliers are the most critical to the success of the company
- Where is the software created, and by whom? What companies create what software that makes up each of the critical products? Where is the data relative to those products stored?
- Who has executed cyber-attacks on us in the past? Who has executed cyber-attacks against others in our industry in the past?
    - List them all out by type, intent, motivation, skill, sophistication, etc.
    - When was the last time each attacked?
    - How many times did each attack?
    - Were they successful?
    - What did they achieve?
    - Did they target any of the IP, PII, or critical products described above?
- What adversaries are most likely to want our intellectual property, and why?
- What adversaries are most likely to want the PII that we hold and why?
- What would adversaries achieve by targeting and exploiting our hardware supply chain?
- What would adversaries achieve by targeting and exploiting our software supply chain?
- What is the current defensive/security posture of the organization?
- What are the SWOTs of that posture? (Strengths, Weaknesses, Opportunities, Threats)
- What gaps do we have in people, process, and technology?

2018 Treadstone 71 LLC

- What is considered the (or are considered) the weaknesses – the least path of resistance in our security stack (people process technology)
- What threat actor attributes would exploit the weaknesses as described above?
- If exploited, what data would the attacker access?
- Who would gain competitively if their nation's hacking apparatus targeted us and shared the fruits of the attack with their like-industries?

The below questions need answering but represent multiple results due to the plural nature. The questions are not individual intelligence requirements.

- Human enacted or directed threats targeting COMPANY systems
- Human enacted or directed threats COMPANY intellectual property
- Human enacted or directed threats source code for theft, destruction, or manipulation
- Human enacted or directed threats COMPANY malware repositories (kind of rolls in with IP)
- Human enacted or directed threats COMPANY, to use COMPANY in a "supply chain" style of attack
- Human enacted or directed threats Adversary/Intelligence repositories (kind of rolls in with IP)
- Human enacted or directed threats COMPANY customers
- Human enacted or directed threats businesses similar to COMPANY
- Human enacted or directed threats tools which COMPANY use, are reliant on, and cannot replace or replicate
- Human enacted or directed threats targeting tools which COMPANY use
- Legal changes or directed which may affect the COMPANY's capability to operate
- Other threat landscape items

Treadstone 71

2018 Treadstone 71 LLC

What makes a good PIR?

A good PIR:

1. Asks a single question
2. Is prioritized and ranked in importance
3. Focuses on a specific event, fact, or activity
4. Is tied to a single decision or planning task that stakeholders have to make
5. Provides a last time by which information is of value (LTIOV – the last possible time we can receive the intelligence report before it is no longer intelligence)
6. Is answerable using available assets and capabilities (existing staff and tools)

The intelligence requirements currently available for this example assessment are the following (NOTE: The *w* IRs below may be replicated for information systems and APT-NAME-ADVERSARY as required after determining those entities likely to target your company (Adversary Threat Matrix)) against COMPANY and CRITICALSYSTEM(s):

PIR#	Priority	Intelligence Requirement
001	##	What COMPANY information system will APT-NAME-ADVERSARY likely target next?
		What initial access technique will APT-NAME-ADVERSARY use next against COMPANY?
		What new defense evasion technique will APT-NAME-ADVERSARY use next against COMPANY?
		How will APT-NAME-ADVERSARY exfiltrate data from the COMPANY HR/Payroll system?
		How will APT-NAME-ADVERSARY exfiltrate data from the COMPANY Payment Gateways?
		How will APT-NAME-ADVERSARY exfiltrate data from the COMPANY MSPs?
		How will APT-NAME-ADVERSARY automate tasks after penetrating the COMPANY HR/Payroll system?
		How will APT-NAME-ADVERSARY automate tasks after penetrating COMPANY Payment Gateways
		How will APT-NAME-ADVERSARY automate tasks after penetrating COMPANY MSPs?
		What would APT-NAME-ADVERSARY do to impact the COMPANY's ability to operate?
		What type of COMPANY intellectual property will APT-NAME-ADVERSARY want most?
		How will APT-NAME-ADVERSARY target COMPANY customer PII?
		How would APT-NAME-ADVERSARY use social media to target COMPANY?
		What mobile device app does APT-NAME-ADVERSARY use to target COMPANY?
		What current CRITICALSYSTEM unpatched vulnerability is likely to be exploited next?
		Is there a zero-day exploit available for the unpatched vulnerability on CRITICALSYSTEM?
		What supply chain software connected to CRITICALSYSTEM is likely to be exploited next?
		How would supply chain software connected to CRITICALSYSTEM be attacked?
		What method could be used to penetrate supply chain software connected CRITICALSYSTEM?

Replication of the following IRs after receiving the crown jewel information:

- What COMPANY HARDWARESUPPLYCHAINLIST target will MALWARE-NAME likely try to exploit?
- What COMPANY SOFTWARESUPPLYCHAINLIST target will MALWARE-NAME likely try to exploit?
- Using the COMPANY as a steppingstone to a CRITICALCLIENTLIST, how would MALWARE-NAME target us to access a CRITICALCLIENTLIST?

As you complete critical organizational asset information, IRs should expand. As the intelligence team builds knowledge on the existing IRs, the data and information collected and analyzed, and the knowledge created is likely to replicate across other IRs.

Treadstone 71

2018 Treadstone 71 LLC

Standard definitions (not in alphabetical order):

Adversary. A party acknowledged as potentially hostile to your organization.

Attributes of Intelligence Excellence (where the measures should be since these are the critical factors for determining maturity in intelligence (CURAT – Complete – Usable – Relevant – Accurate – Timely)).

Anticipatory. Intelligence must anticipate your primary stakeholder's informational needs first based on a clear understanding of critical organizational assets. Anticipation provides the foundation for operational planning and decision-making. Anticipating stakeholder intelligence needs requires the intelligence organization to fully understand current and potential critical organizational assets, the primary stakeholders' intent, all relevant aspects of the operational environment, and all possible adversary TTPs and CoAs. Most important, anticipation requires the aggressive involvement of intelligence in planning at the earliest time possible.

Timely. Intelligence must be available when the stakeholders require it. Timely intelligence enables the stakeholders to anticipate events in the operational area. In turn, this enables stakeholders to time operations for maximum effectiveness and to avoid being surprised. Usually, the need to balance timeliness and completeness should favor timeliness, and if incomplete, should be stated in the product and followed up later. Recognizing and balancing the subtle differences relative to timeliness and completeness is a necessary art form for good intelligence.

Accurate. Intelligence must be factually correct, relay the situation as it exists, and provide an understanding of the operating environment based on the rational judgment of available information. This judgment should evaluate the possibility of an adversary's denial and deception effort. Placing proportionally greater emphasis on information reported by the most reliable sources enhances intelligence product accuracy. Evaluate source reliability through a feedback process in which past data received from a source compares with "ground truth" (for example, when subsequent events or information confirm the source's accuracy).

Usable. Tailor intelligence to the stakeholder's specific needs and provided in forms suitable for immediate comprehension. Providing useful intelligence requires its producers to understand the decisions facing stakeholders, the relevance and impact of intelligence on those decisions, and how to deliver the intelligence to stakeholders in context to balance efficiency and effectiveness. Stakeholders operate under time constraints that shape their intelligence requirements and determine how much time they have to study the intelligence provided. They must quickly apply intelligence and may not have sufficient time to analyze complex intelligence reports. Therefore the "bottom line" must be upfront and understandable; oral presentations should be direct and approved terms used to convey intelligence effectively.

Complete. Complete intelligence answers the stakeholder's questions about the adversary and other aspects of the operating environment to the extent possible and informs stakeholders of significant intelligence gaps. Complete intelligence must identify relevant aspects of the operating environment that may impact the organization and critical organizational assets and offer alternative analysis. Complete intelligence informs stakeholders of all major CoAs available to the adversary and identifies those assessed as most likely and the highest threat level. While providing available intelligence to those who need it

2018 Treadstone 71 LLC

when they need it, we must give priority to stakeholders unsatisfied critical requirements. Intelligence organizations must anticipate and respond to stakeholders existing and contingent intelligence requirements by evaluating the intelligence process input and output surrounding their needs.

Relevant. Intelligence must be relevant to the needs of the organization and aid stakeholders in making decisions. It must contribute to stakeholder's understanding of the adversary and other significant aspects of the operating environment but not burden stakeholders with intelligence that is of minimal or no importance to the current mission.

Objective. Due to the decisive and consequential impact of intelligence on operations and reliance on planning and operations decisions on intelligence, we must maintain objectivity and independence in developing assessments. When informing stakeholders, we must be vigilant in guarding against biases that shade, slant, or frame assessments to favor the chosen CoAs or fit preconceived notions. Intelligence should recognize each adversary as unique and avoid mirror imaging while realizing the possible bias in their assessment type. For example, current intelligence and threat intelligence estimates may assess the same indicators differently. Red teams check analytical judgments by ensuring assumptions about the adversary are sound, and intelligence assessments help minimize mirror imaging and cultural bias.

Available. Intelligence must be readily accessible to stakeholders. Availability is a function of timeliness and usability and appropriate security classification, interoperability, and connectivity. We must strive to provide information at the most appropriate level of classification, thereby maximizing stakeholders' and other consumers' access while protecting sources of information and collection methods.

Basic Intelligence (Baseline-Foundational-Research). Fundamental intelligence concerning the general situation, resources, capabilities, or areas used as reference material in understanding adversaries helps define threats to the organization.

Intelligence. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning hostile or potentially hostile forces or elements or areas of actual or potential operations.

Intelligence Requirement (IR). Any subject, general or specific, upon which there is a need for collecting information or the production of intelligence. A requirement for intelligence to fill a gap in organizational knowledge or *understanding of the operational environment or threat actors.* During baseline intelligence studies, CTI Team identifies significant information gaps about the adversary and other relevant aspects of the operating environment supporting situational awareness.

Priority Intelligence Requirement (PIR). An intelligence requirement stated as a priority for intelligence support that stakeholders need to understand the adversary or the operational environment. Things the commander must know about threat actors to make decisions. PIRs focus on the adversary (TTPs) and the operational environment driving collection. *Intelligence requirements designated as PIRs receive increased intelligence support and priority in allocating resources, while those not designated as PIR are satisfied as time and resources allow.*

Concept of Operations (CONOPS). A verbal or graphic statement clearly and concisely expressing what your primary stakeholder intends to accomplish with available resources.

2018 Treadstone 71 LLC

Information Requirements. In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment need to be collected and processed to meet stakeholders' intelligence requirements.

Indicators. Indicators are positive or negative evidence of threat activity or any characteristic of the adversary that points toward tactics, techniques, procedures, methods, CoA, or any particular threat activity that may influence stakeholders' selection of their CoA.

Essential Elements of Information (EEI). EEIs further refine IRs/PIRs into areas of collected information.

Specific Information Requirements (SIRs). SIRs ease tasking by matching requirements to the capabilities of the collectors/researchers driving mission management.

Requests for Information (RFIs). Stakeholders and intelligence team members may submit RFIs to generate intelligence collection efforts. RFIs are specific, time-sensitive, ad hoc requirements for intelligence information to support an ongoing crisis or operation and not necessarily related to standing requirements or scheduled intelligence production. RFIs fulfill stakeholder requirements and range from disseminating existing products through integrating or tailoring on-hand information to scheduling new collection and production (data determined to be a gap). Collection management translates the stakeholder's requirement determining how best to meet the defined needs. The RFI is assessed against existing knowledge to determine gaps as previously stated. All such information should be timely, accurate, and in a usable format.

Intelligence Collection Plan. A plan for gathering information from all available sources to meet an intelligence requirement. Specifically, a logical plan for transforming the essential elements of information into orders or requests to sources within a required time limit.

Course of Action (CoA). Any sequence of activities.

Intelligence Discipline. A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources.

Intelligence Estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition to determine the CoAs' open to the adversary and the order of probability of their adoption.

Intelligence Preparation of the Cyber Battlespace. An analytical methodology is employed to reduce uncertainties concerning the adversary, the operational environment, and attack surfaces associated with the organization. Intelligence preparation of the cyber battlespace builds an extensive data store for each potential adversary area of operation relative to the organization. The data is then analyzed in detail to determine the adversary's impact, capabilities, and TTPs, and presents it in graphic form. Intelligence preparation of the cyber battlespace is a continuing process.

STEMPLES Plus. Schedule an effort to revisit the STEMPLES Plus documents (Strategic intelligence that helps estimate) to localize STEMPLES Plus specific to your organization. Contextually aligned with the IRs and COMPANY needs. Indicators of Change relate to each item in STEMPLES Plus. Regardless, a timeline that fits delivery of 6-12 months should be placed on each once the IRs are well developed, collection and analysis performed, and information collected that could satisfy some of the indicators of change within the STEMPLES Plus documentation.

2018 Treadstone 71 LLC

Social	Technological	Economic	Military
Political	Legislative	Educational	Security (homeland)
PLUS	Demographics	Religious	Psychological (Hofstede)
Other			

Warning Intelligence. Cyberspace threat intelligence includes analysis to factor in strategic, operational, tactical, and technical intelligence as a warning intelligence report. 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 short time available to respond. These factors make the inclusion of cyber and threat intelligence analysis very important for effectively assessing adversaries' intentions in cyberspace.

The intelligence requirements development (Figure 3 below) outlines the flow defining intelligence requirements through specific information requirements. The flow serves to define collection activities. Activities that become standard as organizational maturity progresses. Gaps in collection should, in time, become smaller in depth and breadth of need.

Treadstone 71

2018 Treadstone 71 LLC

Critical Organizational Asset Assessment versus Country Level Adversary – Measures – SAMPLE ADVERSARY TARGETING MATRICES

Critical Organizational Assets												
Adversary Country	System 1	System 2	System 3	System 4	System 5	Supplier 1	Supplier 2	Supplier 3	MSP1	MSP2	Capability	Potential Impact
North Korea	0	0	0	0	0	0	0	0	0	0	Level 6	Emergency
Russia	4	0	0	0	0	0	0	0	0	0	Level 5	Severe
China	6	0	0	0	0	0	0	0	0	0	Level 4	High
Iran	2	0	0	0	0	0	0	0	0	0	Level 3	Medium
Pakistan	0	0	0	0	0	0	0	0	0	0	Level 2	Low
India	0	0	0	0	0	0	0	0	0	0	Level 1	Unknown
Turkey	0	0	0	0	0	0	0	0	0	0	Level 2	Low
Israel	0	0	0	0	0	0	0	0	0	0	Level 3	Medium
Syria	0	0	0	0	0	0	0	0	0	0	Level 4	High
Islamic State - ISIS	0	0	0	0	0	0	0	0	0	0	Level 5	High
Al-Qaeda	0	0	0	0	0	0	0	0	0	0	Level 6	Severe

Figure 4 Sample Adversary Threat Matrix against Company Critical Assets by Nation-State

Level of Concern	
6	Serious Concern
4	Subsantial Concern
2	Moderate Concern
1	Low Concern
0	Negligible Concern

Treadstone 71

2018 Treadstone 71 LLC

Capability

Level 1	The cyber actor(s) possess extremely limited technical capabilities and largely make use of publicly-available attack tools and malware. Sensitive data supposedly leaked by the attackers are often linked back to previous breaches and publicly-available data.
Level 2	Attackers can develop rudimentary tools and scripts to achieve desired ends in combination with the use of publicly-available resources. They may make use of known vulnerabilities and exploits.
Level 3	Actors maintain a moderate degree of technical sophistication and can carry out moderately-damaging attacks on target systems using a combination of custom and publicly-available resources. They may be capable of authoring rudimentary custom malware.
Level 4	Attackers are part of a larger and well-resourced syndicate with a moderate-to-high level of technical sophistication. The actors are capable of writing custom tools and malware and can conduct targeted reconnaissance and staging prior to conducting attack campaigns.
Level 5	Actors are part of a larger and well-resourced organization with high levels of technical capabilities such as those exhibited by Level 4 actor sets. In addition, Level 5 actors have the capability of introducing vulnerabilities in target products and systems, or the supply chain, to facilitate subsequent exploitation.
Level 6	Nation-state supported actors possessing the highest levels of technical sophistication reserved for only a select set of countries. The actors can engage in full-spectrum operations, utilizing the full breadth of capabilities available in cyber operations in concert with other elements of state power, including conventional military force and foreign intelligence services with global reach.

Potential Impact

Unknown	
Low	Damages from these attacks are highly unlikely or are unable to adversely affected the targeted systems and infrastructure. Such incidents may result in minor reputational damage. Sensitive systems and data remain intact, confidential, and available.
Medium	Attacks have the capacity to disrupt some non-critical business functions, and the impact is likely intermittent and non-uniform across the user-base. User data and sensitive information remain protected.
High	Attacks have the potential to disrupt some core business functions, although the impact may be intermittent and non-uniform across the user-base. Critical assets and infrastructure remain functional, even if they suffer from moderate disruption. Some non-sensitive data may be exposed. Actors at this level might also expose sensitive data.
Severe	Cyber-attacks emanating from this actor set have the capacity to disrupt regular business operations and governmental functions severely. Such incidents may result in the temporary outage of critical services and the compromise of sensitive data.
Emergency	Kinetic and cyber-attacks conducted by the threat actor(s) have the potential to cause complete paralysis and/or destruction of critical systems and infrastructure. Such attacks have the capacity to result in significant destruction of property and/or loss of life. Under such circumstances, regular business operations and/or government functions cease and data confidentiality, integrity, and availability are completely compromised for extended periods.

Treadstone 71

2018 Treadstone 71 LLC

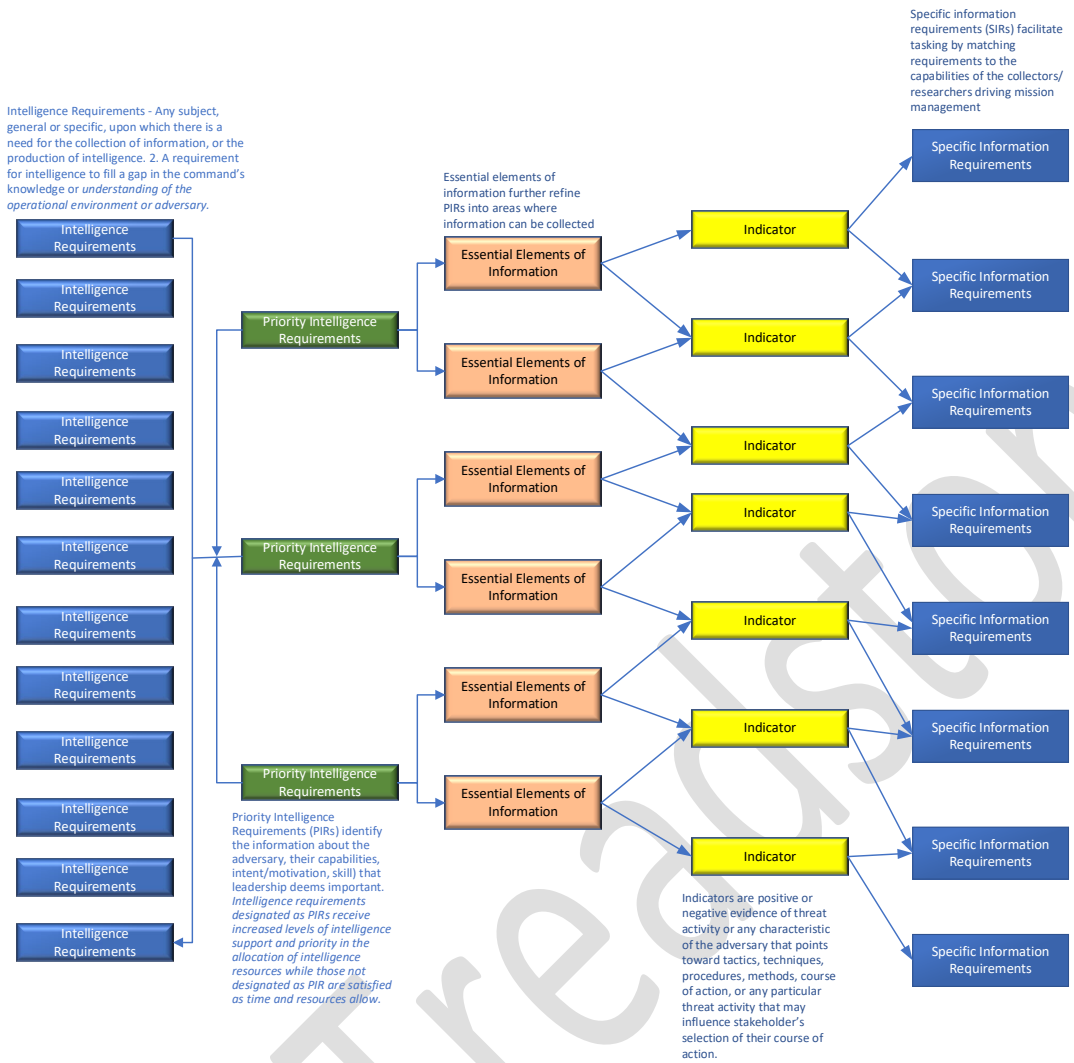


Figure 5 Intelligence Requirements Flow

Treadstone 71

2018 Treadstone 71 LLC