Autor: José Luis Martínez Rodríguez

Fecha: Mayo 2025

Comparación de inteligencia militar e inteligencia de amenazas en ciberdefensa

En el mundo militar, especialmente en el ámbito de la inteligencia militar, las interrogantes del comandante se denominan formalmente “Requerimientos de Información del comandante o CCIR que viene de su sigla en inglés “Commander’s Critical Information Requirements.

Pero que son los CCIR y por que los comparo con la inteligencia de amenazas de ciberseguridad, bueno como se explicó en la clase, la mayoría si es que no todas las técnicas usadas están basadas o tiene sus inicios en su uso militar, y es por este motivo que les prepare este documento que les puede ayudar a comprender un poco mejor los conceptos y como usarlos en sus empresas o trabajos.

Los CCIR son todas aquellas preguntas claves que un comandante de unidad necesita que se respondan para tomar decisiones informadas especialmente en el contexto militar, y luego podemos proyectar ese razonamiento hacia la ciberdefensa que es la materia de este curso.

Entonces ¿Por qué los CCIR permiten tomar decisiones informadas?

1. Reducción de la incertidumbre en un entorno caótico: El campo de batalla, sea físico o cibernético, sabemos y debemos esperar que este lleno de información incompleta, ambigua o incluso falsa. Es por este motivo que el comandante no puede esperar a tener "todo claro" para actuar, y los CCIR le ayudan a enfocar la recolección de inteligencia (información necesaria para cumplir la misión), que realmente sea relevante para la misión, evitando sobrecarga de datos.

Decidir sin información clave = Se toman decisiones de manera improvisada.

Decidir con información priorizada = Se actúa o toma decisiones estratégicamente.

2. Priorización de recursos limitados: Tropas, vehículos, comunicaciones, sistemas de armas, tiempo de vigilancia aérea: todo es limitado. Los CCIR permiten al comandante asignar esos recursos en función de lo que realmente necesita saber.

Ejemplo militar: Si un PIR indica que el enemigo tiene una batería antiaérea en cierto punto, se puede reprogramar un reconocimiento aéreo para confirmar eso antes de enviar una operación de helicópteros.

Ejemplo ciberdefensa: si la inteligencia de amenazas identifica que la vulnerabilidad CVE-2024-XXXX está siendo explotada activamente por grupos APT contra tecnologías VPN similares a las que usa la organización, esa información permite tomar una decisión informada antes de ejecutar acciones operativas críticas. Así, se puede suspender el despliegue de una nueva aplicación expuesta a internet, activar un escaneo de vulnerabilidades urgente, ajustar reglas del WAF para bloquear intentos de explotación y escalar la alerta al CISO.

3. Alineación entre inteligencia y operaciones: Los CCIR sirven como un puente entre el G2 (inteligencia) y el G3 (operaciones) en una unidad militar. Esto ayuda a que la inteligencia no trabaje en el vacío, sino en función directa de las necesidades tácticas del comandante.

Sin CCIR: la inteligencia produce reportes generales.

Con CCIR: la inteligencia se enfoca en lo que cambia el curso de la misión.

4. Facilitan decisiones bajo presión: En combate, muchas decisiones se toman bajo tiempo limitado y presión extrema, y en un SOC o CSIRT, si se está recibiendo o controlando un incidente de seguridad se actúa bajo presión por lo que tener un marco previo (CCIR) permite que cuando llega nueva información crítica, ya se sepa qué significa y qué se tomen acciones y decisiones adecuadas.

Ejemplo: “Si se confirma que el puente ha sido volado por el enemigo (PIR), entonces el plan de avance se desvía a Ruta Bravo automáticamente.”

Proyección a Ciberdefensa

En ciberseguridad, donde millones de eventos ocurren cada segundo y los equipos SOC están saturados de alertas, la formulación de CCIR/PIR/FFIR cibernéticos cumple el mismo propósito:

Rol militar	Equivalente ciber
Comandante de unidad	CISO o jefe de SOC
Campo de batalla	Red, endpoints, activos críticos
CCIR	¿Qué amenazas pueden afectar directamente mi infraestructura crítica ahora?
Decisión táctica	¿Activamos contención, informamos, elevamos alerta?

En resumen, los CCIR no son una lista de "cosas interesantes de saber". Son herramientas decisionales críticas que:

- Disminuyen la incertidumbre
- Enfocan la atención en lo que tiene valor operativo
- Alinean inteligencia con acción
- Agilizan la respuesta bajo presión

Y estos están estrechamente relacionadas con el proceso de planificación y ejecución de misiones y se dividen típicamente en las siguientes categorías:

PIR (Priority Intelligence Requirements)

Información que el comandante necesita saber sobre el enemigo, el entorno o posibles amenazas.

Ejemplo militar: "¿Dónde está ubicada la unidad de artillería enemiga?", esta se responde mediante inteligencia de amenazas, ISR (Intelligence, Surveillance & Reconnaissance), HUMINT, y otras siglas o métodos de uso militar.

Ejemplo de ciberdefensa: "¿Qué grupo APT está actualmente llevando a cabo campañas dirigidas contra sistemas SCADA en infraestructuras energéticas similares a las nuestras?", esta pregunta nos permite anticipar ataques específicos a sistemas industriales críticos, activar vigilancia especial, ajustar reglas en IDS/IPS, aplicar parches urgentes o incluso activar protocolos de contingencia antes de un incidente.

FFIR (Friendly Force Information Requirements)

Información relacionada con el estado, ubicación y capacidades de las propias fuerzas.

Ejemplo militar: “¿Ha cruzado ya nuestra unidad avanzada el río Bravo?”, esto se responde con reportes internos, logística, comunicaciones operacionales.

Ejemplo de ciberdefensa: “¿Están completamente desplegadas y operativas las actualizaciones de seguridad en los firewalls perimetrales y sistemas VPN críticos?”, esta pregunta nos permite validar que la infraestructura de defensa está lista para resistir amenazas identificadas en PIRs, evitando puntos débiles internos que puedan ser explotados. Si se descubre una brecha como, por ejemplo, un firewall desactualizado, se puede detener un cambio operativo, elevar la alerta o priorizar medidas correctivas inmediatas.

EEFI (Essential Elements of Friendly Information)

Información interna que debe protegerse para evitar que sea explotada por el adversario.

Ejemplo militar: “¿Qué unidades de comunicaciones están desplegadas en la zona sur y qué frecuencias están utilizando?”, si el enemigo accede a esta información, podría lanzar interferencias electrónicas o jamming, interceptar transmisiones o realizar ataques de guerra electrónica, por eso esta información se debe protege mediante cifrado, compartimentación, rotación de frecuencias y contramedidas electrónicas.

Ejemplo en ciberdefensa: “¿Dónde están almacenadas las copias de seguridad y cuáles son las credenciales administrativas que permiten su restauración?”, si un actor de amenazas, como un Ransomware o una APT accede a esta información, puede eliminar las copias antes de cifrar el sistema, anulando cualquier plan de recuperación ante incidentes, por ello esta información se protege mediante control de acceso estricto, cifrado, separación física o lógica de redes, y principios de Zero Trust.

Se debe de mencionar que a diferencia del PIR (que busca información del enemigo) y del FFIR (que evalúa nuestro estado operativo), el EEFI se enfoca en lo que el enemigo no debe saber nunca. Su gestión adecuada es parte esencial de la seguridad operacional y del plan de contrainteligencia.

Ahora ¿Por qué los CCIR son clave en ciberdefensa?, en operaciones de ciberdefensa, los CCIR permiten:

- Enfocar los esfuerzos de inteligencia cibernética.
- Priorizar acciones defensivas o contraofensivas.
- Asignar recursos en base a la criticidad de activos o amenazas.

Ejemplo aplicado a ciberdefensa.

Tipo	**Interrogante del comandante**
PIR	¿Qué APT está apuntando a nuestros sistemas de mando y control?
FFIR	¿El equipo azul ha restaurado completamente la retransmisión de comunicaciones?

Aplicación de los CCIR y PIR a la Inteligencia de Amenazas Cibernéticas

1. Analogía y adaptación

Comandante = CISO, jefe de SOC o director de Operaciones

Campo de batalla = Red empresarial o infraestructura crítica

Adversario = APTs, grupos criminales, Ransomware, etc.

CCIR/PIR/FFIR = Preguntas clave que el CISO o analista de amenazas necesita responder para proteger, contener y anticipar ataques

2. Ejemplos de uso de PIR en ciberseguridad

Categoría	**Ejemplo de PIR (Requerimiento Prioritario de Inteligencia)**
Actor	¿Qué TTPs usa el grupo APT29 contra infraestructura OT?
Infraestructura	¿Se han detectado conexiones salientes al dominio C2 xyz.ru en nuestra red?
Vulnerabilidad	¿Estamos expuestos a la CVE-2024-xxxx que explota el servicio VPN?

Impacto	¿Qué activos críticos podrían ser afectados si se compromete nuestro AD?
Tiempo	¿Qué ventana temporal se anticipa para una acción adversaria relacionada con elecciones?

3. Flujo práctico en un equipo de Threat Intelligence

1.- Formulación de PIR (ej. ¿Qué amenazas afectan nuestro sector?)

↓

2.- Recolección de datos (OSINT, feeds, MISP, honeypots)

↓

3.- Análisis (MITRE ATT&CK, campaña, actor, CVEs)

↓

4.- Producción de inteligencia (informe táctico/estratégico)

↓

5.- Toma de decisiones (bloqueos, alertas, inversiones, políticas)

El flujo práctico en un equipo de Threat Intelligence sirve para organizar el ciclo completo de gestión de inteligencia de amenazas, asegurando que la información recolectada sea relevante, procesada, accionable y útil para la defensa de la organización. Este flujo permite transformar datos crudos (como IoCs, TTPs, alertas, logs) en decisiones operativas y estratégicas, alineadas con las prioridades del negocio o misión (como los PIR/CCIR).

¿Cómo se usa este flujo?

1. Formulación de requerimientos (PIR/FFIR): Se definen las preguntas clave que se deben responder como, por ejemplo: "¿Qué APTs están activos en nuestro sector?", esto nos ayuda a focalizar la búsqueda y evita perder tiempo en datos irrelevantes.

2. Recolección de datos: Se recopila información desde múltiples fuentes: OSINT, inteligencia comercial (threat feeds), análisis internos, honeypots, logs de SIEM, etc.

3. Análisis: Se evalúa la confiabilidad, contexto y severidad de los datos recopilados luego se correlacionan, por ejemplo, dominios maliciosos con campañas conocidas, y se enriquecen usando frameworks como MITRE ATT&CK.

4. Producción de inteligencia: Se redactan informes tácticos para el SOC, operacionales para el CSIRT o estratégicos para CISO o alta dirección, esto puede incluir: IoCs, TTPs, recomendaciones, cursos de acción, etc.

5. Difusión y uso: La inteligencia se usa para reforzar defensas, por ejemplo, bloquear IPs, ajustar reglas en SIEM o en los firewalls, además se deben compartir los hallazgos relevantes con otras áreas o alianzas (ISACs, CERTs).

6. Retroalimentación: El equipo operativo informa sobre la efectividad respondiendo preguntas como ¿el IOC fue útil? ¿el ataque fue contenido? y se ajusta el enfoque para futuras investigaciones.

Este flujo sirve para:

- Convertir información en decisiones defensivas.
- Aumentar la velocidad y precisión de respuesta.
- Priorizar recursos en lo que realmente importa.
- Anticipar amenazas antes de que impacten.
- Informar la estrategia de ciberseguridad con base real.

Veamos un contexto simulado que pude servir de quia:

Entidad: Centro de Operaciones de Ciberdefensa Nacional

Activos críticos: Infraestructura de mando y control, sistemas SCADA, red de comunicaciones satelitales

Amenazas: APT extranjeros, Ransomware dirigido, insiders, hacktivismo

Apliquemos una matriz para identificar los PIR / FFIR para inteligencia de amenazas cibernéticas

Tipo	Requerimiento	Relación MITRE ATT&CK	Objetivo de Ciberdefensa
PIR	¿Qué APT está activo actualmente en nuestra región y qué TTPs emplea contra sistemas de defensa?	TTPs: Reconocimiento, Persistencia, movimiento lateral.	Preparar reglas de detección y caza de amenazas
PIR	¿Qué campañas de malware están usando ingeniería social para comprometer cuentas militares?	Phishing (T1566)	Fortalecer entrenamiento y filtrado de correo, instrucción de usuarios sobre prevención de Phishing.
PIR	¿Hay explotación activa de CVEs recientes en nuestro perímetro (VPN, Exchange)?	Exploitation of Public-Facing App (T1190)	Aplicar parches prioritarios y monitoreo
PIR	¿Qué dominios o IPs están actuando como C2 para malware dirigido a sistemas OT?	C2 Channel (T1071), Proxy (T1090)	Bloquear y alertar en perímetro
FFIR	¿El segmento clasificado de la red ha mantenido la integridad y no hay actividad anómala?	–	Verificación de contención, respuesta rápida
FFIR	¿Las actualizaciones de seguridad han sido aplicadas a todos los nodos del sistema de comunicaciones satelital?	–	Hay que asegurar que no existan brechas conocidas
FFIR	¿El equipo azul ha detectado indicadores coincidentes con amenazas identificadas?	–	Verificar que la inteligencia ha sido operacionalizada
FFIR	¿La red de simulación de entrenamiento ha sido segmentada correctamente del entorno real?	–	Prevenir fuga o entrada accidental de amenazas

Como podemos usar esta matriz básica:

Se deben generar a partir de un análisis de amenazas y riesgos.

Su revisión y actualización debe realizarse de manera diaria, semanal, o según se disponga o se determine en el SOC/CERT/CSIRT.

Las preguntas son guías para la recolección de inteligencia, casería de amenazas, y tareas del equipo técnico, se pueden formular tantas preguntas como interrogantes existan.

Cada respuesta obtenida genera un informe táctico o estratégico y activa la toma de decisiones de ciberdefensa.

Ejemplos en el área militar:

PIR: ¿Qué tipo de armamento posee la unidad blindada enemiga al este del río?

PIR: ¿Cuál es la intención del enemigo en las próximas 48 horas en el eje norte?

FFIR: ¿Ha llegado la brigada aliada al punto de reunión Bravo?

FFIR: ¿Se mantiene operativa la red de comunicaciones tácticas de la división?

EEFI: ¿Cuál es el plan de repliegue si el enemigo toma la colina 412?

Ejemplos en ciberdefensa:

PIR: ¿Qué APTs están atacando sistemas SCADA en el sector energía actualmente?

PIR: ¿Qué nuevas TTPs se observan en campañas de phishing contra personal gubernamental?

FFIR: ¿Están actualizados y operativos los sistemas de defensa perimetral WAF, IDS, Firewall u otros?

FFIR: ¿El segmento crítico de red interna se mantiene aislado del resto de la infraestructura?

EEFI: ¿Cuáles son los protocolos de restauración ante ataques de Ransomware en entornos clasificados?

Glosario de términos:

Sigla	Significado	Descripción Funcional
APT	Advanced Persistent Threat	Ataque sostenido y sofisticado, típicamente dirigido por un Estado o grupo bien financiado.
CCIR	Commander's Critical Information Requirements	Preguntas clave que el comandante necesita responder para tomar decisiones.
PIR	Priority Intelligence Requirements	Información prioritaria sobre el enemigo o entorno que se debe conocer.
FFIR	Friendly Force Information Requirements	Información crítica sobre el estado o capacidades propias.
EEFI	Essential Elements of Friendly Information	Información sensible propia que debe mantenerse fuera del alcance del adversario.
IOC	Indicator of Compromise	Evidencia técnica de actividad maliciosa (hash, IP, dominio, etc.).
C2	Command and Control	Canal que usa un malware para comunicarse con su atacante.
SCADA	Supervisory Control and Data Acquisition	Sistema que monitorea/controla infraestructuras industriales.
WAF	Web Application Firewall	Firewall específico para proteger aplicaciones web.
IDS	Intrusion Detection System	Detecta actividades sospechosas o ataques en una red.
EDR	Endpoint Detection and Response	Detección y respuesta en dispositivos finales.
XDR	Extended Detection and Response	Detección extendida integrando múltiples capas: red, endpoint, email, etc.
SIEM	Security Information and Event Management	Consolida eventos de seguridad para detección y análisis.

SOAR	Security Orchestration, Automation and Response	Automatiza y coordina respuesta ante incidentes.
OSINT	Open Source Intelligence	Inteligencia basada en fuentes públicas (web, redes, etc.).
HUMINT	Human Intelligence	Inteligencia obtenida a través de fuentes humanas.
IMINT	Imagery Intelligence	Inteligencia basada en imágenes satelitales o aéreas.
SIGINT	Signals Intelligence	Inteligencia a partir de la intercepción de señales.
MASINT	Measurement and Signature Intelligence	Inteligencia a través de análisis técnicos (firmas térmicas, sónicas, etc.).
IR	Incident Response	Respuesta ante incidentes de seguridad.
TIP	Threat Intelligence Platform	Plataforma para gestionar y distribuir inteligencia de amenazas.
MITRE ATT&CK	Adversarial Tactics, Techniques & Common Knowledge	Framework de técnicas y tácticas de ataque usadas por adversarios.
CTI	Cyber Threat Intelligence	Inteligencia específica sobre amenazas cibernéticas.
DLP	Data Loss Prevention	Tecnología que evita la fuga de información confidencial.
VPN	Virtual Private Network	Red privada virtual para comunicaciones seguras.
FTP	File Transfer Protocol	Protocolo para transferir archivos. A veces usado maliciosamente.
TTP	Tactics, Techniques and Procedures	Conjunto de patrones observables usados por adversarios.
Kill Chain	Cyber Kill Chain	Modelo en fases para entender y prevenir ciberataques.
Zero Trust	–	Modelo que no confía en ningún usuario o sistema por defecto.
RaaS	Ransomware as a Service	Ransomware vendido como servicio a través del mercado negro.
MaaS	Malware as a Service	Alquiler de kits de malware a través de foros o redes.
PaaS	Pay-per-Install (PpiS)	Servicio de instalación maliciosa a cambio de pago por víctima.
TaaS	Translation as a Service	Servicios de traducción para campañas maliciosas específicas.
MlaS	Money Laundering as a Service	Servicio de lavado de dinero vinculado al cibercrimen.

Recon	Reconnaissance	Fase de reconocimiento inicial de objetivos.
Weaponization	–	Creación del malware o exploit personalizado.
Delivery	–	Envío del malware al objetivo (correo, web, USB, etc.).
Exploitation	–	Ejecución del exploit o apertura del vector de entrada.
Installation	–	Instalación del malware en el sistema víctima.
Action on Objectives	–	Fase en que se cumple el objetivo: robo, sabotaje, etc.