InFo-Cyber. Journal of Cybersecurity and Digital Forensics.
Volumen 1, Número 1. Año 2026. ISSN: en trámite.
https://revistas.ufasta.edu.ar/index.php/InFoCyber/index

INFO-CYBER CYBERSECURITY AND DIGITAL FORENSICS JOURNAL

Vehículo táctico de acción inmediata ante incidentes en el ciberespacio (2025)

Tactical vehicle for immediate action in response to incidents in cyberspace (2025)

Agustín Perciavalle

UFASTA, Buenos Aires (Argentina)

agustin.percia@hotmail.com

https://orcid.org/ 0009-0007-5908-827X

Artículo de investigación

Recibido: 02-09-2024. Aceptado: 02-10-2025
Publicado: 03-03-2026

Universidad FASTA. Facultad de ingeniería; Mar del Plata, Argentina

Resumen

Enmarcados en el contexto del siglo XXI, los enfrentamientos bélicos han evolucionado a pasos agigantados en diversos aspectos, especialmente en el plano tecnológico. Dichas conflagraciones suelen enfrentar a oponentes dispares, conformando conflictos asimétricos e híbridos. Esta situación trae aparejada la necesidad de incorporar nuevas tácticas operacionales con sus correspondientes doctrinas y herramientas.

En los escenarios de combate, solo se emplean sistemas de guerra electrónica, orientados a la intervención y bloqueo del espectro comunicacional. Sin embargo, no se utilizan de manera integral las funcionalidades emergentes desde el dominio digital, como la inteligencia artificial aplicada al combate o el uso de la informática forense.

Durante el desarrollo de este trabajo de investigación, se llevó a cabo un relevamiento de diferentes vehículos, aplicaciones y sistemas tecnológicos aplicados al ámbito de la ciberguerra.

A raíz de ello, se propone la creación de un laboratorio informático móvil de acción inmediata ante incidentes en el ciberespacio, bautizado como VLAIC (vehículo liviano de análisis, investigación y ciberdefensa). El diseño se organiza en torno a tres módulos principales que permiten una operación integral y especializada: área de investigación, sector de electrónica operativa y un módulo dedicado al análisis forense digital.

Como herramienta estratégica en el dominio cibernético, este rodado con capacidades de DFIR presenta una alta versatilidad, permitiendo su despliegue en tiempos de guerra o paz. Tal es el caso de tareas de asistencia a infraestructuras críticas —ya sean civiles o militares— ante la ocurrencia de un ciberataque, constituyendo un claro ejemplo de aplicación en contextos no bélicos.

Teniendo en cuenta la constante evolución tecnológica, es fundamental incrementar las capacidades y medios existentes en el ámbito de la ciberdefensa. Es por ello que se plantea dotar de esta capacidad (hoy inexistente) a las Fuerzas Armadas argentinas y lograr situarlas en un nivel que permita afrontar los nuevos desafíos tecnológicos mundiales.

Palabras clave

ciberdefensa, conflictos asimétricos e híbridos, laboratorio informático móvil

Abstract

In the context of the 21st century, military conflicts have evolved rapidly in various aspects, especially in terms of technology. These conflicts often pit disparate opponents against each other, creating asymmetric and hybrid conflicts; this situation brings with it the need to incorporate new operational tactics with their corresponding doctrines and tools.

In this regard, combat scenarios only employ electronic warfare systems aimed at intervening in and blocking the communications spectrum. However, emerging functionalities from the digital domain, such as artificial intelligence applied to combat or the use of computer forensics, are not used comprehensively.

During the course of this research, a survey was conducted of different vehicles, applications, and technological systems applied to the field of cyberwarfare. As a result, the creation of a mobile computer laboratory for immediate action in response to incidents in cyberspace, called VLAIC (light vehicle for analysis, investigation, and cyber defense), is proposed. The design is organized around three main modules that allow for comprehensive and specialized operation: research area, operational electronics sector, and a module dedicated to digital forensic analysis.

As a strategic tool in the cyber domain, this vehicle with DFIR capabilities is highly versatile, allowing it to be deployed in times of war or peace. Such is the case with critical infrastructure assistance tasks—whether civilian or military—in the event of a cyberattack, constituting a clear example of application in non-war contexts.

Given the constant technological evolution, it is essential to increase existing capabilities and resources in cyber defense. That is why there are plans to provide this capability (which does not currently exist) to the Argentine Armed Forces and bring them up to a level that will enable them to face new global technological challenges.

Keywords

asymmetric and hybrid conflicts, cyber defense, mobile computer lab

AGUSTÍN PERCIAVALLE es especialista en Informática Forense egresado de UFASTA y en Seguridad, Higiene y Protección Ambiental, entre otras disciplinas que posee. Es perito informático oficial, docente, investigador y Oficial de Reserva del Ejército Argentino, incorporado en la Compañía de Reserva de Buenos Aires. Su labor profesional se enfoca en el análisis forense digital, cibercrimen, ciberdefensa y el desarrollo de capacidades tecnológicas aplicadas al ámbito militar, incluyendo el diseño de soluciones basadas en inteligencia artificial para entornos operativos y de respuesta rápida.

I. Introducción

La génesis de esta investigación nace de una iniciativa propia ideada en el año 2018, a raíz de una carencia detectada en las Fuerzas Armadas argentinas, puntualmente expuesta en el dinamismo de operaciones de ciberdefensa durante contiendas armadas y fuera de ellas.

Por esta razón, se evaluó la factibilidad de instaurar un vehículo dotado de capacidades de ciberguerra, con el objetivo de ser desplegado dentro y fuera del país, brindando apoyo ante posibles operaciones ofensivas, defensivas y de exploración.

A lo largo de estos siete años, se realizaron tareas de campo, análisis de bibliografía y testeo de *software* y *hardware* forense [1, p. 76]. Todo este material, conformado por fuentes primarias y secundarias, facilitó la confección de un análisis a nivel local e internacional.

Fig. 1. Vista exterior de un prototipo del VLAIC realizada mediante IA.

Como etapa inicial, se evaluaron diferentes vehículos, herramientas y equipos informáticos. En una etapa secundaria, se testeó el funcionamiento de los mismos, en especial el rendimiento de las fuentes de energía del sistema vehicular. Todo ello permitió, en una última etapa, realizar una propuesta final del prototipo y anexarle múltiples capacidades que serán analizadas en las siguientes páginas.

Vale la pena aclarar que el trabajo completo fue desarrollado, a su vez, como Trabajo Final Integrador en una carrera de posgrado, y, por lo tanto, lo plasmado en este escrito representa solo una síntesis del mismo.

En suma, a lo analizado y a los fines de lograr dichas metas, se propone la creación de una nueva capacidad militar, para así acompañar el impulso tecnológico vivido en esta era. Resulta de vital interés, el hecho de que este proyecto pueda ser evaluado por el Estado argentino e implementado mediante un prototipo a desarrollar.

II. Ciberdefensa y Geopolítica

A. *Descripción de la problemática.*

En los últimos años, autores como Klaus Schwab y Wolfgang Wahlster han sostenido que la humanidad transita una cuarta revolución industrial. En la mayor parte de sus aspectos, estos cambios han aportado mejoras a la sociedad, aunque también han generado nuevas formas de disidencia en las relaciones humanas [2].

Recurriendo al ámbito de los conflictos armados, se ha podido apreciar en las últimas décadas distintas conflagraciones que enfrentaron oponentes dispares. Es decir, hubo combates asimétricos e híbridos que se libran en distintos escenarios y situaciones donde fuerzas armadas regulares se enfrentan a oponentes no organizados, tales como paramilitares, reservistas, mercenarios, etnias religiosas y demás grupos armados. Prueba de ello son los hechos ocurridos en Ucrania, Afganistán, Irak, Palestina, Siria, entre otros conflictos recientes.

Respecto a las comunicaciones que se suscitan en las rivalidades actuales, se observa que las diversas facciones no detentan en su haber equipos de comunicación militar, radares, computadoras militares y satélites. Aquellos son reemplazados por medios civiles, tales como teléfonos celulares, computadoras, tabletas digitales, drones, relojes inteligentes, etc. Estos cambios de paradigma en el aspecto comunicacional generan que aplicaciones de mensajerías y redes sociales estén presentes hoy en cualquier conflicto armado.

Asimismo, esta situación de escasez se puede contemplar hoy en día, inclusive en fuerzas armadas regulares. Tal es el caso del Ejército ruso desplegado en Ucrania que, ante la falta de equipos de comunicaciones militares, utiliza telefonía móvil.

La informática es una de las ciencias que mayor incremento denota en lo que refiere a hostilidades, especialmente en la temática relacionada con la seguridad informática. Según Gabriel Baca Urbina [3, p. 10], la misma se trata de una "disciplina que, con base en políticas y normas internas y externas de la organización, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático contra cualquier tipo de amenaza". Se destaca, en esta noción, la amplitud con la que el escritor explaya este concepto, pudiendo incluir dentro del mismo concepciones como la seguridad física de una sala de servidores mediante control biométrico.

Si bien la literatura internacional suele referirse al concepto de *cyberwarfare* (ciberguerra), en el ámbito nacional se ha adoptado el término Ciberdefensa. Esta elección no implica una limitación a operaciones exclusivamente defensivas, sino que responde a la necesidad de enmarcar dichas actividades dentro

de las competencias y funciones propias del Ministerio de Defensa.

Inserto en este marco, se incorpora el concepto de ciberataque, definido como "la acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan" [1, p. 203]

En la actualidad, los ciberataques han registrado un incremento significativo, generando daños cada vez mayores e incurriendo en implicancias que abarcan otros sectores, tales como el energético y el sanitario. Gran parte de estos ataques fueron dirigidos a estructuras civiles y gubernamentales, alcanzando su máximo nivel de hostilidad en las infraestructuras críticas, es decir, aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente [4, anexo 2, p. 10], existiendo o no un conflicto declarado. Como resultado de ello, las naciones han debido replantear su rol y estructura de las fuerzas armadas en el devenir de los años.

Para complementar las ideas expuestas anteriormente, resulta necesario confeccionar algunas aclaraciones sobre el marco legal en el cual se incluyen los ciberataques. Los mismos se pueden encontrar bajo la órbita del Ministerio de Seguridad o del Ministerio de Defensa. El primero actúa en caso de amenazas de naturaleza criminal, mientras que el segundo está encargado de repeler ataques de naturaleza militar (siendo difícil detectar los mismos, ya que se los suele enmascarar a través de otras organizaciones privadas o ciberactivistas).

No obstante, pueden ocurrir situaciones donde un ataque informático sea de origen incierto, o peor aún, sea atribuido a un tercero sin ser este el emisor. Ocasiones tales como las producidas por el ciberterrorismo provocan choque de competencias entre los dos ministerios, pudiendo actuar las Fuerzas de Seguridad a través de CSIRT y las Fuerzas Armadas mediante su Comando de Ciberdefensa.

Asociado a esta noción, aparece el concepto de infraestructuras críticas de la información [4, anexo 1, p. 1], que relaciona los aspectos de comunicación que resultan vitales para el funcionamiento de las infraestructuras críticas. Por último, el concepto de infraestructura crítica del instrumento militar se refiere a sistemas de comando y control, sistema de armas, sistemas de control, sistema de comunicaciones y sistemas informáticos.

En cuanto al ámbito militar local, es conveniente recalcar la dificultad que el mismo atraviesa, debido a la poca disponibilidad de recursos humanos especializados, costo de equipos informáticos y licencias, extensión geográfica y ausencia de hipótesis de conflicto. Para mayor entendimiento, se recomienda al lector indagar en la doctrina geopolítica de planeamiento por capacidades versus planeamiento por hipótesis de conflicto [5].

Adicionalmente, sucede que la migración de personal militar hacia el ámbito civil (empresas) aumenta año tras año, dificultando la capacitación continua y permanencia del mismo en el progreso de nuevas habilidades. De igual manera, otra causante que incrementa la problemática es la deficiente normativa en materia de ciberdefensa, la cual no ha logrado aggiornarse al dinamismo tecnológico. Por consiguiente, las Fuerzas Armadas argentinas (FF.AA.) no han absorbido la creciente demanda de desafíos en el ámbito tecnológico y en especial informático, impactando en mayor o menor medida en la adecuación de nuevas capacidades.

Sin embargo, cabe destacar que la mayoría de estos problemas también trascienden la frontera nacional. Si bien las diferentes naciones han perfeccionado sus recursos informáticos en materia de ciberdefensa, no han logrado aún una rápida respuesta ante incidentes informáticos. Esto sucede debido a la falta de movilidad para resolver situaciones parcial o totalmente *in situ*, ocasionando impactos negativos, tales como la demora en la resolución ante un daño.

B. *Investigación preliminar*

Según lo recabado a nivel local durante las investigaciones realizadas, no se halló dentro del parque automotor de las FF.AA. ningún equipo dotado con capacidades de ciberdefensa. En base a ello, se llevaron a cabo tareas de campo en distintos organismos y empresas, para conocer la disponibilidad de recursos y evaluar la factibilidad de este proyecto a nivel nacional.

En los Estados Unidos de América, la empresa Lockheed Martin posee la concesión para desarrollar un prototipo de vehículo apto para guerra electrónica, capaz de controlar el espectro electromagnético [6]. Este desarrollo se localiza sobre el chasis de un vehículo blindado de combate a rueda [7] llamado Stryker [8], el cual provee opciones de guerra cibernética, bloqueo, interferencia de comunicaciones y apoyo al comandante, brindando una comprensión mayor del entorno electrónico del campo de batalla. Este rodado puede generar señales capaces de evitar detonaciones activadas por radio e interrumpir señales de radiofrecuencia. El blindado, en la actualidad, se encuentra en etapa experimental y realizatareas de apoyo en diversos teatros de operaciones [9].

Las Fuerzas Armadas rusas poseen un vehículo diseñado sobre la base de un camión de gran tamaño, el cual también tiene capacidades de guerra electrónica [10] y fue bautizado como Krasukha. Su rol consiste en emitir radiación electromagnética para anular sensores enemigos, falsificación de señales GPS y todas las características citadas en el vehículo norteamericano. Este rodado es útil contra drones, helicópteros, aviones, radares de vigilancia, misiles, etc. En cuanto a su alcance, el mismo abarca entre 100 y 300 km. En la actualidad, se encuentra en actividad en la contienda frente a Ucrania y se lo puede visualizar operando en cercanía de distintas ciudades.

Con respecto a las opciones internacionales, tanto el rodado americano como el ruso no representan, bajo ningún punto de vista, similitud alguna con lo planteado en este trabajo de investigación, ya que ambos son utilizados con fines de guerra electrónica. En lo estructural, el Stryker [11] es un vehículo blindado y el Krasukha, camión de grandes proporciones, ambos de tamaño superior al buscado para el laboratorio móvil. Estos rodados de poca movilidad cuentan con una velocidad de traslado reducida en comparación con otros de su misma clase.

Como conclusión a este apartado, las búsquedas realizadas acerca de la existencia de un centro de comando móvil con capacidades de ciberdefensa a nivel nacional e internacional fueron negativas [12], no hallándose información publicada que permita asegurar la existencia de un vehículo con las características ideadas.

C. *Propuesta*

Durante esta investigación se formularon una serie de propuestas que pudieran mitigar la problemática planteada, culminando con la elección de una de ellas: un vehículo táctico de acción inmediata ante incidentes en el ciberespacio, con capacidades de DFIR. Este concepto integra la respuesta a incidentes y análisis forense, permitiendo reforzar las capacidades hoy existentes, apoyando al instrumento militar terrestre y dotando de información al órgano rector de decisiones.

Uno de los principales fuertes del proyecto radica en que, al tratarse de una unidad móvil, puede conformarse como equipo de respuesta rápida y ser trasladado a distintos sitios donde se hayan suscitado ataques informáticos a infraestructuras críticas. Aunque, por otro lado, puede desempeñarse de manera estacionaria como laboratorio, permaneciendo en el sitio donde se lo destine orgánicamente, reforzando capacidades operativas y educativas en las FF.AA.

III. Elección del vehículo

La alternativa presentada implica el uso de un vehículo para operaciones ofensivas, defensivas, exploratorias y control de daños. A modo introductorio, se pueden mencionar algunos de los ejes básicos en cuanto al diseño y funcionalidad del VLAIC:

- Ejecución del proyecto sobre vehículo de fabricación nacional o importado
- Uso de *software* libre y licenciado
- Disponibilidad de diversas herramientas y hardware
- Múltiples fuentes energéticas
- Posibilidad de acelerar la resolución de contingencias y obtención de información
- Traslado hacia la zona de conflicto permitiendo realizar triage (análisis en el lugar del hecho)
- Implementación de tres sectores dentro del vehículo: investigación, electrónica y análisis forense. [3]

A. *Estructura y diseño del laboratorio móvil*

A los fines de dotar al vehículo de movilidad y versatilidad, fue preciso analizar distintos modelos de blindados a rueda. Las orugas (cadenas que reemplazan a las ruedas) [13] requieren mayor mantenimiento, y en caso de tener que substituir algunas partes de la misma, no resulta tan sencillo como sí sucede en el caso de una rueda. Asimismo, un transporte a rueda logra mayor velocidad y estabilidad en la cabina, y menor daño en infraestructura vial pública.

1. Tracción

En esta temática, resulta indispensable la utilización de tracción 4x4, ante la necesidad de soportar toda clase de suelos y accidentes geográficos. La amortiguación y suspensión deben ser acordes a la tracción instalada, pudiendo trasladarse en montaña, vadear arroyos, transitar terreno arcilloso, entre otros [14].

2. Temperatura

La Argentina posee biomas y temperaturas de las más diversas. Por este motivo, es fundamental en la estructura del VLAIC contar con un sistema de refrigeración exclusivo para la cabina, que permita enfriar los equipos informáticos allí instalados. En lo referente a calefacción, la misma ya viene incluida de fábrica en todos los vehículos; por ende, no es necesario adicionar un sistema exclusivo.

3. Tripulación

Se proyecta una dotación de siete tripulantes: conductor, radioperador/tirador, radarista/tirador, perito n.º1/jefe de grupo, perito n.º 2, auxiliar de inteligencia y técnico electrónico [15].

Respecto a la tripulación de cabina, la misma se conforma por un técnico electrónico que trabaja sobre dispositivos IoT [16] , así como también brinda apoyo respecto a las fuentes de energía en el VLAIC. En segundo lugar, los dos peritos informáticos se encargan de dispositivos móviles, computadoras y redes. Finalmente, en cuanto a la presencia de un auxiliar de inteligencia, su tarea es la obtención de información en fuentes abiertas y la inspección del contenido de evidencia digital obtenido por los peritos[5].

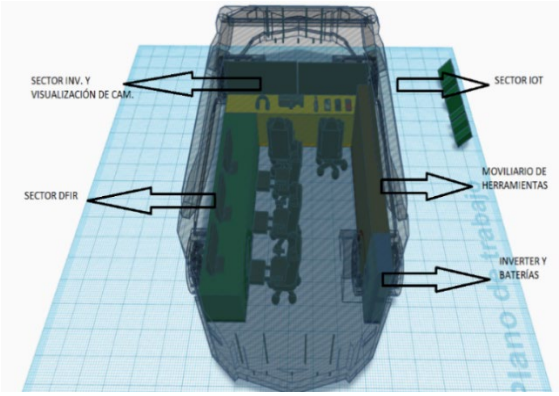

Fig. 2. Sectores operativos de la unidad DFIR.

B. Comunicaciones

A nivel comunicacional, se procura incorporar un equipo que se posee en dotación: Harris Falcon II RF-580V-MP. Se trata de una radio que opera en banda de frecuencia de 30 MHz a 108 MHz con cifrado de tipo CITADEL o AES y un sistema de GPS. El propósito de contar con un equipo de radio es transmitir información obtenida o requerida al puesto comando o al centro integrador, con el fin de que, a su vez, sea retransmitida a las unidades presentes en el teatro de operaciones; y viceversa.

C. Prototipos evaluados

En base a las especificaciones de diseño y estructura, se seleccionaron tres variables de vehículos que cumplen con lo requerido: Bushmaster MR6, Alvis Glover Táctica y Grupcom-R.

Fabricado en Australia por la empresa Thales, el Bushmaster MR6 [18], posee un excelente diseño de chasis, tecnología, blindaje, suspensión, comunicaciones, protección antiminas y capacidad de tripulantes. A su vez, se trata de una unidad probada en combate que se fabrica desde 1997, habiendo generado diversas versiones y mejoras con el correr del tiempo, habiendo prestado servicio en Afganistán, Irak, Mali, Israel, Siria y recientemente en Ucrania.

En segunda instancia, el 4x4 Alvis Glover Táctica [19] posee un diseño netamente militar y con un interior rústico, no contando con tecnología actualizada. La Argentina dispone de ocho unidades adquiridas en el año 1998, las cuales fueron destinadas a misiones de paz, replegándose a suelo argentino en el 2018. Esta opción, representa como ventaja la disminución en el costo del proyecto, así como la disponibilidad de personal militar ya entrenado en el uso y mantenimiento del mismo.

Fig. 3. Vista exterior del prototipo Grupcom-R, de Interservit.

De fabricación nacional, el "Grupcom-R" de la empresa argentina Interservit [20], prototipo creado hace tres años, presenta varias de las características requeridas esbozadas anteriormente. Como ventaja, se puede mencionar su fabricación nacional y mantenimiento en los talleres de Interservit. Respecto a las desventajas, el diseño del Grupcom-R es en su mayoría orientado a un entorno urbano; por lo tanto, en cuanto a equipamiento de tecnología, diseño militar, vías de escape y potencia, es ampliamente superado por las dos variables analizadas anteriormente.

Luego de cotejar las características y estructura de las tres opciones, se puede concluir que el Grupcom-R representa la opción favorita por su costo y mantenimiento. Sin embargo, en relación al factor seguridad y equipamiento, sin duda el Bushmaster MR6 es el adecuado, para el caso en que se disponga de mayor presupuesto.

D. Sistema energético

El montaje de un laboratorio móvil requiere la necesidad de disponer de manera ininterrumpida y constante a la demanda de distintos equipos informáticos. Por ende, es preciso contar con diversas fuentes de energía, las cuales puedan alternarse y concatenarse. Siguiendo una política amigable con el medioambiente, se propone la inclusión de energías renovables, sobre las bases de la norma ISO 50001[21] de eficiencia energética.

Para comenzar, una de las ventajas de contar con diversos tipos de energía es la de encontrarse en aptitud de conectar distintos equipos, recargar drones y VANTS (vehículos aéreos

no tripulados) [22] y complementar puestos de comunicaciones, entre otros. Como fuentes de obtención energética, se pueden citar: batería propia del vehículo, banco de baterías náuticas e inversor, panel solar, alargue de conexión a 220V de 50 metros y grupo electrógeno.

E. Equipamiento informático forense

Para la confección de este apartado, fue de utilidad la experiencia laboral adquirida a lo largo de los años en tareas de cibercrimen, informática forense y ciberdefensa. Dichas operaciones fueron realizadas tanto de manera estacionaria en un laboratorio como en vehículos destinados a otros fines. Complementaron esta experiencia las simulaciones realizadas en entornos controlados en ámbito universitario.

Respecto del equipamiento con que cuenta una unidad móvil, es similar al de cualquier otro laboratorio informático forense. Sin embargo, al estar montado sobre un vehículo ideado para operaciones dinámicas, los tiempos de trabajo se reducen a su mínima expresión. De allí la necesidad de contar con hardware y *software* de gran *performance*.

Alusivo a herramientas de hardware, se testearon: bloqueadores, duplicadores, notebooks, servidores, estaciones de trabajo forense, inhibidores de señal, kits de electrónica y equipos UFED de la empresa Cellebrite [23]. Referido a *software*, se trabajó con Encase, Axiom, Griffeye, Tableau Image r[24], FTK, UFED 4PC y Analyzer.

Fig. 4. Imagen de duplicadores marca Tableau modelos TD2, TD3 y TX1.

En cuanto al *software* analizado, el mismo está conformado por el conjunto de herramientas *open source* y licenciadas, que tienen por finalidad cumplir las misiones asignadas. Algunas de esas tareas son: informática forense, telefonía, investigación, escaneo de vulnerabilidades, *hasheo* [25], procesamiento y análisis de información, análisis de DVR, volcado de memoria, versiones *triage*, *sniffing*, distribuciones de Linux y aplicaciones para generar distintos ciberataques.

F. Herramientas

Resulta indispensable contar con un maletín de herramientas, conformado por destornilladores y pinzas de varios tipos y tamaños, junto con un kit de electrónica adaptado para pequeños dispositivos. A su vez, es útil contar con un set de Arduino, con el fin de perpetrar simulaciones, instalar y/o reemplazar piezas deficientes en los objetivos a analizar.

En referencia al sector destinado a IoT dentro del laboratorio móvil, se contempla la existencia de herramientas y accesorios para a cometer distintas tareas de ingeniería inversa, tales como *chip off*, *j-tag* e ISP. Todo ello se hace con el fin de realizar extracciones forenses en el caso de que los dispositivos a peritar lleguen dañados o no sea posible obtener información por métodos convencionales. Se complementan dichos activos con equipos de mayor tamaño, tales como estación de soldado, osciloscopio, fuente regulada, multímetro, pulsera y manta antiestática.

En caso de actuar en el marco de la justicia argentina, habiendo sido víctima de algún ciberataque, se debe preservar la evidencia digital y asegurar la trazabilidad de la cadena de custodia. Para ello, es fundamental poseer bolsas y precintos numerados de diferentes tamaños a los fines de resguardar la evidencia obtenida [26].

Idealmente, se pretende contar con bolsas de Faraday utilizadas para resguardar dispositivos móviles. El material de estas bolsas forma un blindaje alrededor de teléfonos celulares, GPS, netbooks, dispositivos *bluetooth*, laptops, etc., bloqueando toda señal celular, wifi o de radio. Las mismas son diseñadas para la recolección, preservación, transporte y análisis de dispositivos móviles e inalámbricos. El dispositivo no podrá volver a conectarse con la red, aunque se halle encendido, asegurando que el mismo no pueda ser controlado, localizado o bloqueado remotamente [27].

IV. CAPACIDADES DEL VLAIC

Dentro del proyecto de laboratorio móvil de DFIR, se sugiere una diversidad de servicios aplicables en distintos escenarios. Un ejemplo de ello es su uso en pleno campo de batalla, como a su vez en un puesto comando (sitio de toma de decisiones) localizado lejos del mismo [28]. En contraposición, alejado del teatro de operaciones o en tiempos de paz, se puede contar con las capacidades de DFIR, para movilizarse a distintos sitios donde se hayan suscitado ataques informáticos a infraestructuras críticas en territorio argentino [29].

En cuanto a las capacidades del proyecto, se pueden mencionar: peritaje de dispositivos, herramientas de ataque y defensa de *malware*, aplicaciones de investigación en fuentes abiertas, bloqueo de redes móviles y *wireless*, estación de recarga de drones, sistema analizador de espectro radioeléctrico, drones, radar, equipo de derribo de drones, entre otras.

Fig. 5. Capacidades del VLAIC. A. Función Ofensiva

Habiendo definido el concepto de ciberataque en las páginas anteriores, se puede ahondar en una categorización formulada a los fines de este trabajo y para facilitar la comprensión de tareas:

—ataques externos (*malware*): suceden sin la interacción con los usuarios víctimas. Por ejemplo, alguna vulnerabilidad descubierta en un sitio web.

—ataques internos (ingeniería social): los agresores precisan acceder a los sistemas o a credenciales de usuarios.

Respecto a los ataques externos, son los más difíciles de perpetrar, y están protagonizados por *malware*, el cual trata de un *software* que ocasiona perjuicios de manera intencionada en un sistema informático, y sin el consentimiento del usuario. Algunas de las categorías más conocidas son: virus, *worms*, *bots*, *spyware*, *rootkit*, troyanos, *fileless malware*, *backdoors*, *keyloggers* y demás técnicas. En relación a los ataques hacia redes informáticas, las técnicas de *sniffing* y ataques basados en el concepto de "*man in the middle*" permitirían interceptar el contenido de los paquetes que se transmiten.

Los vectores de ataques internos son más habituales, ya que la cadena se rompe siempre por el eslabón más débil (usuario, operador, empleado). Este tipo de ataque resulta más sencillo debido a que no se necesita eliminar barreras de seguridad como *firewalls*, *IDS*, antivirus, etc. Algunas de las técnicas son: *pishing*, sim *swapping*, BEC, *smishing*, *baiting*, entre otros.

Utilizando los datos obtenidos mediante la informática forense y la investigación digital, se pueden generar distintos tipos de ataques, teniendo como objetivo infraestructuras críticas y blancos militares. Para ello, se generan operaciones sobre la red informática enemiga, junto con operaciones de guerra electrónica; a los fines de dañar o interrumpir las comunicaciones e infraestructura del enemigo (esto comúnmente es llamado operaciones de información).

Uno de los pilares más importantes de estas operaciones es la función de "comando y control del enemigo", es decir, eliminar el centro de toma de decisiones (donde se encuentre la plana mayor, órgano rector que dispone sobre la operación militar) [30]. Si bien existe la alternativa de destrucción física, lograr eliminar sus comunicaciones y que no pueda recibir ni enviar órdenes a sus subalternos, garantiza una alta efectividad.

Es útil recordar que un ciberataque puede afectar satélites, comunicaciones, servicios y demás infraestructuras, ya sea inutilizándolos o generando un mal funcionamiento que arroje falsos positivos. Esto no solo afecta al servicio en sí, sino que perjudica los sistemas de navegación terrestres, marítimos y aéreos.

Fig. 6. Ciclo de medidas realizadas por el VLAIC ante un ataque informático. B. Función Defensiva

Para iniciar con este tópico, es conveniente reflexionar sobre lo siguiente: ¿es importante la inversión en medidas ofensivas y defensivas en ciberdefensa? Si bien es afirmativa esta respuesta, quizás lo más importante sea la velocidad con la que se recupera una infraestructura luego de recibido el ataque. Y, por otro lado, igualmente relevante resulta cómo se rastrea la amenaza para poder eliminarla o conocer el origen de la misma.

A los fines de proteger una infraestructura de red ya existente, se puede desplegar personal especializado a bordo del vehículo, con la finalidad de instalar *software* adicional o efectuar pruebas de penetración en el objetivo a proteger. Esto se realiza mediante un escaneo de puertos y análisis de vulnerabilidades para conocer el estado actual de la red.

La incorporación de dispositivos de análisis forenses de red permite capturar paquetes sin pérdidas de datos, no solo respecto a los históricos, sino en tiempo real. Mediante estos equipos se logra: información de seguridad y gestión de eventos, detección y respuesta de red, análisis de tráfico de red y sistema de detección de intrusos. Esto es aplicable tanto para infraestructuras civiles como militares, y permite analizar, controlar y responder ante diversos ataques informáticos.

Bajo un criterio preventivo en la gestión de incidentes, una de las capacidades del VLAIC es la de realizar tareas de *pentesting*. Ello se representa mediante una auditoría de seguridad informática, previamente pactada y coordinada, para

analizar la situación actual del objetivo preestablecido. Esta actividad conforma la tarea de evaluar el estado de un sistema informático. Luego de ello, se escanean las vulnerabilidades y a posteriori, se verifican los impactos negativos. Finalmente, se generan medidas de contingencia y mitigación ante los impactos identificados [31].

Esta auditoría puede efectuarse con el finde hallar vulnerabilidades propias o ajenas, conformando finalmente operaciones defensivas u ofensivas. En cuanto a su materialización, puede implementarse de manera virtual, presencial o mixta. Es importante poder desarrollar medidas preventivas, en base a los riesgos encontrados, para reducir el impacto futuro, aplicando luego el concepto de mejora expuesto en el SGSI (sistema de gestión de seguridad de la información) [32].

A. Informática Forense

Se trata de una disciplina en auge que constituye uno de los pilares fundamentales de la ciberdefensa y, por ende, es una capacidad de suma importancia en el laboratorio móvil. Dicha especialidad representa la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar evidencia digital. [1, p. 76]

Por evidencia digital, se entiende a la información de interés en formato digital (código binario), la cual está almacenada en un dispositivo físico. Incluye los metadatos, archivos de varios tipos, conexiones de red, discos rígidos, memorias, internet de las cosas, etc. Este análisis muchas veces se remite a tareas en la *deep web*, redes p2p, nube, sitios web estándar.

Para organizar las labores, se propone que el interior del rodado esté dividido en tres subespecialidades: dispositivos móviles, equipos informáticos y electrónica aplicada e IOT.

B. Dispositivos móviles

Se considera de esta manera a todos los periféricos de pequeño tamaño, que en su mayoría ostentan una serie de características en común, tales como no precisar conexión permanente a la red eléctrica, conexión a internet, sistema operativo o firmware, memoria RAM, CPU y almacenamiento interno/externo. Esta descripción incluye a los drones, celulares, relojes inteligentes, tablets, robots, dispositivos IoT, VANTS, robots terrestres y náuticos.

Para efectuar extracciones forenses a estos dispositivos, es importante contar principalmente con la herramienta UFED (Cellebrite), la cual es la más completa existente hoy en día en el mercado en dicha materia. No solo por sus continuas actualizaciones en cuanto a modelos de dispositivos, sino por la gran cantidad de complementos de *hardware* que posee.

Si bien existe una variedad de licencias y servicios que ofrece UFED, resulta relevante poder referir al menos tres clases de distribuciones. En los equipos de escritorio, la versión UFED4PC y Analyzer es suficiente para las tareas de este laboratorio. Por otro lado, la versión UFED Analytics desktop Panasonic se puede utilizar dentro del vehículo, así como fuera del mismo. Esto se realiza trasladando la valija rígida hacia el sitio que se desee, ya que cuenta con una protección adecuada y batería suficiente. Por último, una tercera versión, UFED Touch II, del tamaño de una tableta digital, la cual permite ser trasladada por algún operador, en caso de que forme parte de alguna misión.

Fig. 7. Testeos realizados durante una extracción de Ufed Touch II y Ufed4PC en laboratorio móvil.

La idea de incorporar la capacidad de extracción forense radica en la posibilidad de poder inspeccionar el contenido de los dispositivos secuestrados. Esto abarca desde teléfonos en poder del enemigo, dispositivos secuestrados durante misiones de paz, móviles incautados en el marco de terrorismo, etc. A partir de su análisis, se puede visualizar conversaciones, lista de contactos, redes sociales, archivos multimedia, *software* instalado y demás información que será de utilidad para actuales y posteriores operaciones militares.

Este mismo equipamiento sirve para ejecutar extracciones en drones capturados al enemigo, inclusive en caso de que hayan sufrido daño alguno. Ya sea a su memoria interna como a la tarjeta expansora que posea, se puede obtener traza de ruta, geolocalización de bases enemigas o punto de partida, contenido multimedia, etc. Esta información no solo sirve para planificar futuras operaciones ofensivas, sino también para analizar vulnerabilidades futuras en el dispositivo secuestrado.

Asimismo, se prevé su eventual recuperación, puesta en condiciones operativas y reutilización por parte de las tropas propias, como recurso complementario en el marco de las operaciones militares.

C. Dispositivos informáticos

Algunas de las actividades operativas a efectuar son la confección de copias forenses, análisis de memoria RAM [33], extracción de información con herramientas *triage* y procesamiento de evidencia digital. Es decir, tal como sucede en telefonía, las tareas pueden cumplirse en el interior del vehículo, o trasladar a los técnicos al lugar del hecho y llevar a cabo el análisis forense "en caliente".

La subespecialidad de "equipos informáticos" permite entre otras cosas: analizar datacenter, extraer información de computadoras, ejecutar revisión de sistema SCADA y HMI, extraer y visualizar cámaras de videovigilancia y otras tareas forenses. Esto con el fin de recopilar información del enemigo, analizar vulnerabilidades, revisar daños ante ataque informático, escanear *malware*, entre otros. Uno de los equipos sugeridos para ello es el Packet Falcon [34] que brinda acceso a análisis de medios de red y captura de paquetes.

D. Electrónica aplicada y la IoT

Otra de las funcionalidades de este VLAIC es el laboratorio de electrónica y dispositivos IoT. Dicha capacidad permite obtener información de dispositivos a los cuales no sería posible efectuarles una forensia convencional. Algunos de los procedimientos que puede realizar esta subespecialidad son: reparación de dispositivos, reemplazo de piezas, rooteo, Jailbreak, herramientas y adaptadores para acceso a datos, JTag, ISP y Chip-Off.

Con dichas técnicas, se amplían las capacidades del laboratorio, al incluir dentro de las posibilidades de obtención de información: distintos sistemas de armas, sistemas de comunicaciones, hardware de misiles y vehículos aéreos no tripulados, hardware de aviones y embarcaciones, radares, entre otras opciones.

E. OSINT

Como analista de información digital, se identifica a la persona encargada de llevar a cabo el análisis de la evidencia digital. Dicho rol no solo se basa en obtener información producto de las pericias informáticas realizadas, sino también en todo el análisis de OSINT que pudiere implementar. Este análisis también es conocido como "inteligencia de fuentes abiertas", el cual representa al conjunto de herramientas y técnicas que permite recopilar y examinar datos, los cuales en su mayoría son públicos, no incurriendo en delito alguno.

A los fines militares, mediante estas técnicas, se puede recopilar información sobre armamento, unidades, cantidad de hombres, infraestructura de red, sistemas operativos, *software* y *hardware*, infraestructuras críticas, bases militares, nombre de comandantes, proveedores de internet de las unidades militares, datos personales, etc.

F. Función de vigilancia

Ante esta perspectiva, se incluye el alistamiento de un radar de corto alcance. En base a los análisis realizados sobre el material de dotación en el Ejército, se selecciona al radar Thales GO 80 [35]. Este tipo de dispositivo posee un alcance de 80 km de reconocimiento, y permite detectar hasta 80 personas en este rango. Facilita también el seguimiento de hasta 50 objetivos en simultáneo en una misma operación [36].

Por otro lado, mediante la incorporación de un sistema de cámaras exteriores e interiores a 360°, se facilita visualizar lo que sucede dentro y fuera de la unidad [37]. Esta acción puede llevarse a cabo desde el interior del laboratorio, mediante una pantalla, así como de manera remota en cualquier sitio del mundo.

Esta tarea puede complementarse con cámaras de visión térmica y nocturna. Dicha funcionalidad aporta valor agregado a las características del VLAIC. Esto se realiza con siete cámaras de vigilancia full HD y dos domos 360°. Con la instalación de un mástil telescópico, se puede lograr mayor amplitud en los sistemas de comunicaciones y vigilancia, así como en los de videofilmación.

Otra utilidad que podría agregarse de manera opcional es la de un sistema analizador de todas las bandas del espectro radioeléctrico, a los fines de poder intervenir comunicaciones. Ello se complementa con la presencia de herramientas de interceptación y localización de dispositivos celulares.

Con la finalidad de aprovechar la cantidad de pantallas disponibles en la cabina, se propone el sincronizado de imágenes con drones y VANTS, desplegados en el terreno con fines de exploración y vigilancia, visualizando dichas imágenes en VLAIC. Para ello se sugiere el M30-T, dron de la marca DJI, que resulta extremadamente versátil para los objetivos perseguidos.

No se descarta la posibilidad de utilizar esta unidad móvil como plataforma de VANTS con fines de ataque; sin embargo, quedará pendiente su análisis para un próximo trabajo de investigación.

V. CONCLUSIÓN

En concordancia con los razonamientos esbozados en las líneas anteriores, y ante el aumento de ataques informáticos, resulta necesario dotar a las FF.AA. de una nueva capacidad de respuesta ante incidentes en infraestructuras críticas civiles y militares. Las mismas requieren celeridad en los tiempos de respuesta, a los fines de recuperar su operatividad en el menor tiempo posible.

Como consecuencia de este escenario dinámico, se propone

la incorporación de un VLAIC, que permita proteger de manera eficiente y precisa a los recursos económicos, naturales y humanos. Inicialmente, comenzando con la fabricación de un prototipo, el cual podrá ser replicado en nuevas unidades. Como veta de este proyecto, y habiendo considerado la ausencia de laboratorios móviles de ciberdefensa en estratos internacionales, es útil contemplar la posibilidad de exportación a otras regiones.

Contar con un laboratorio informático móvil con capacidades de DFIR pone en avanzada al aparato militar argentino. Pudiendo actuar en operaciones ofensivas y defensivas, en múltiples escenarios, sobrepasando en aptitudes a los países limítrofes y estando en igualdad de condiciones frente a cualquier potencia militar del primer mundo.

Parte del equipamiento disponible en el interior del móvil se encuentra representado por herramientas forenses y electrónicas, equipos de comunicaciones, drones y otros dispositivos. Los mismos, junto a la utilización de *software* especializado, permiten el peritaje de dispositivos, diagrama de operaciones, investigaciones, análisis del espectro radioeléctrico y otros atributos con los que cuenta esta unidad.

Por consiguiente, es indispensable la generación de energía capaz de abastecer a los equipos informáticos. Para ello se propuso contar con fuentes diversas que aseguren disponer de energía de manera ininterrumpida, entre ellas la posibilidad de contar con un panel solar.

Finalmente, la propuesta innovadora presentada no solo establece un marco avanzado para fortalecer las capacidades de ciberdefensa, sino que también abre las puertas a nuevas estrategias y tecnologías emergentes. Este enfoque vanguardista no solo capacita a las fuerzas militares para enfrentar los desafíos tecnológicos actuales, sino que también los prepara para anticipar y adaptarse a las amenazas del futuro, garantizando así una defensa robusta y resiliente en el siglo XXI.

Referencias

[1] CCN, C. C. (agosto de 2015). Guía de Seguridad (CCN-STIC-401), Glosario y Abreviaturas. [En línea]. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-determinos/22-401-descargar-glosario/file.html

[2] C. Clark, "Write algorithms, wage EW, share data: Lessons from Ukraine war", *Breaking Defense*, 30 may. 2023. [En línea]. Disponible: https://breakingdefense.com/2023/05/write-algorithms-wage-ew-share-data-lessons-from-ukraine-war/

[3] G. Baca Urbina, *Introducción a la seguridad informática*, 1a ed. México: Grupo Editorial Patria, 2016.

[4] Jefatura de Gabinete de Ministros, Secretaría de Gobierno de Modernización. 12 de septiembre del 2019. Resolución 1523/2019. Glosario de términos de ciberseguridad. [En línea]. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

[5] Ministerio de Defensa España, *Entorno operativo 2035*, 2019.

[6] C. Plott y J. Keller, "Cyber and Electromagnetic Activities (CEMA) Operations Impacts on Human Performance Final Report", U.S. Army CCDC Data & Analysis Center, vol. 1, pp. 1-59, ene. 2020.

[7] Ejército Argentino, *RF - 99 – 01. Terminología de uso castrense en el Ejército Argentino*. Buenos Aires: Departamento Doctrina, 2001.

[8] Patrascu, D. 19 de octubre, 2021. Autoevolution. U.S. Army Tactical Vehicles to Get New Cyber Warfare Capabilities. [En línea]. Disponible en https://www.autoevolution.com/news/us-army-tactical-vehicles-to-get-new-cyber-warfare-capabilities-172046.html

[9] Ejército Argentino, *RC - 11 – 99. Diccionario para la acción militar conjunta*. Buenos Aires: Departamento Doctrina, 1999.

[10] Pelletier, J. 1 de marzo, 2022. Intelligence, information warfare, cyber warfare, electronic warfare – what they are and how Russia is using them in Ukraine. The conversation. [En línea]. Disponible en https://theconversation.com/intelligence-information-warfare-cyber-warfare-electronic-warfare-what-they-are-and-how-russia-is-using-them-in-ukraine-177899

[11] I. Bisht, "US Army Unveils Ground Vehicle Cyber Attack Protection", *The Defense Post*, 10 feb. 2022. [En línea]. Disponible: https://www.thedefensepost.com/2022/02/10/us-army-vehicle-cyber-attack/

[12] J. Trevithick, "Army Hires Company to Develop Cyber Defenses for Its Strykers After They Were Hacked", *The Warzone*, 17 nov. 2020. [En línea]. Disponible: https://www.thedrive.com/the-war-zone/37684/army-hires-company-to-develop-cyber-defenses-for-its-strykers-after-they-were-hacked

[13] Ejército Argentino, *ROP – 04 – 06. Sección de Ingenieros orgánica de la Subunidad de Ingenieros perteneciente al Batallón de Ingenieros Liviano*. Buenos Aires: Departamento Doctrina, 2006.

[14] Ejército Argentino, *RFP 00 – 10. Estudio Geográfico Militar*. Buenos Aires: Departamento Doctrina, 2001.

[15] Ejército Argentino, *ROB - 11 – 01. Conducción para el instrumento militar terrestre*. Buenos Aires: Departamento Doctrina, 2001.

[16] IBM. (S.f.). [En línea]. Disponible en https://www.ibm.com/mx-es/topics/internet-of-things

[17] S. Kent, *Inteligencia Estratégica*, 2da ed. Buenos Aires: Editorial Pleamar, 1978.

[18] Thales. (s.f). Bushmaster. [En línea]. Disponible en www.thalesgroup.com/en/global/presence/asiapacific/australia/defence/bushmaster

[19] Rivas, S. Pucara defensa. (s.f.). [En línea]. Disponible en https://www.pucara.org/post/la-iii-divisi%C3%B3n-del-ej%C3%A9rcito-argentino-muestra-el-equipo-de-algunas-de-sus-unidades

[20] Interservit. (s.f). Industria de la defensa. [En línea]. Disponible en http://www.interservit.com.ar/industria-de-defensa

[21] *Sistemas de gestión de la energía*, Norma ISO 50001:2011. [En línea]. Disponible: https://www.energia.gob.ar/contenidos/archivos/Reorganizacion/eficiencia_energetica/1introducionygeneralidades.pdf

[22] H. Gomez, "Usos, alcances y limitaciones de los sistemas de información en tiempo real en el teatro de operaciones", Trabajo Final Integrador, Esc. Sup. de Guerra Conjunta de las FF.AA., 2012. [En línea]. Disponible en www.cefadigital.edu.ar/bitstream/1847939/274/1/TFI%20342012%20GOMEZ.pdf

[23] Cellebrite. (s.f). UFED. [En línea]. Disponible en https://cellebrite.com/es/pagina-principal/

[24] Digital Intelligence, "Tableau Forensic TX1 Imager". [En línea]. Disponible: https://digitalintelligence.com/files/TX1_User_Guide.pdf

[25] *Normativa para el análisis e interpretación de evidencias digitales*, Norma ISO/IEC 27042:2015. [En línea]. Disponible: https://peritosinformaticos.es/iso-27042-perito-informatico/

[26] Ministerio Público Fiscal y Ministerio de Seguridad, *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*, 2023.

[27] *Lineamientos para la identificación, la recolección, la adquisición y la preservación de la evidencia digital*, Norma IRAM-ISO/IEC 27037:2022, Buenos Aires: IRAM. [En línea]. Disponible: https://www.iram.org.ar/

[28] Ejército Argentino, *ROB 00-01. Conducción para las Fuerzas Terrestres*. Buenos Aires: Departamento Doctrina, 2015.

[29] Subsecretaría de Tecnologías de la Información, Jefatura de Gabinete de Ministros, *Guía de Notificación y Gestión de Incidentes de Ciberseguridad*, 16 jun. 2023.

[30] Ejército Argentino, *RC 12 – 01. Inteligencia para la acción militar conjunta*. Buenos Aires: Departamento Doctrina, 2007.

[31] A. Di Iorio, P. Cistoldi y B. Constanzo, *Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense*, 1a ed. Mar del Plata: Universidad FASTA, 2019.

[32] *Sistemas de gestión de la seguridad de la información*, Norma IRAM-ISO/IEC 27000 y subsiguientes, Buenos Aires: IRAM. [En línea]. Disponible en https://www.iram.org.ar/

[33] A. Di Iorio, M. Castellote y B. Constanzo, *El rastro digital del delito, aspectos técnicos, legales y estratégicos de la informática forense*, 1a ed. Mar del Plata: Universidad FASTA y REUP, 2017.

[34] Neox Networks. (s.f). NEOX Packet Falcon. [En línea]. Disponible en https://www.neox-networks.com/en/products/neox-networks/portable-network-capturing-neox-packet-falcon/

[35] Ejército Argentino, Batallón de Comunicaciones 602, "Radares y comunicaciones". [En línea]. Disponible: https://somosea.mil.ar/index.php/com_vig/

[36] Ejército Argentino, *ROD - 11 – 01. Inteligencia Táctica*. Buenos Aires: Departamento Doctrina, 2007.

[37] Ejército Argentino, *ROP – 11 – 06. Medidas de seguridad de contrainteligencia*. Buenos Aires: Departamento Doctrina, 2006.