Ciberespacio: 660 días de observación. Proyecto Observatorio Argentino del Ciberespacio (OAC)

Cyberspace: 660 days of observation. Argentine Cyberspace Observatory Project (OAC)

ALEJANDRO A. MORESI, CARLOS AMAYA, ALEJANDRA CASTILLO
Escuela superior de Guerra Conjunta,
Universidad de la Defensa Nacional, Argentina
alejandro.moresi@conjunta.undef.edu.ar

El artículo presenta una síntesis de la actividad llevada a cabo por el Observatorio Argentino del Ciberespacio (OAC) desde su creación, durante casi 2 años de actividad continua de observación de un ambiente virtual. Esta observación es relativamente nueva para la humanidad y la cual muestra un exponencial crecimiento en la cantidad de personas que a él acceden, así como el tiempo que ellas dedican al mismo. Hasta no hace mucho, el ciberespacio era objeto de un limitado empleo para comunicarse y realizar algunas tareas puntuales. Hoy, prácticamente todas las actividades del mundo real se realizan en él: desde las relaciones sociales y de trabajo, hasta la aparición de deportes virtuales, entretenimiento, investigación y estudio. La pandemia lo ha llevado al centro de la escena para todas las actividades humanas, sean

estas personales, familiares, educativas y/o sociales. La propuesta, más allá de tratar la evolución del OAC, intenta mostrar cómo ha sido la interacción y articulación con la sociedad y el medio, comentar las lecciones aprendidas y las estrategias observadas por quienes operan allí, analizando el impacto de las tecnologías que lo componen y, finalmente, dar pautas para su continuidad.

1. El proyecto y sus comienzos

Origen del proyecto

A partir de la detección de una falencia en lo académico y social respecto de las problemáticas de ciberdefensa y ciberseguridad, la Escuela Superior de Guerra Conjunta estudió diferentes alternativas de mitigación del problema: dedicar horas de clase al alumnado, realizar exposiciones magistrales, armar seminarios en la materia, entre otras. Todas ellas eran adecuadas y posibles, pero no reunían el objetivo de permanencia y continuidad en la tarea.

Así surgió la idea de crear un observatorio. Esa posibilidad permitía acceder a una amplia gama de sectores sociales: la comunidad académica y educativa, las áreas especializadas y también la sociedad en general. Esta metodología permitiría llegar de manera permanente a diferentes estadios sociales con la actualidad del *"estado del arte en la materia".* Además, en caso de contar con la adecuada financiación, podría desarrollar actividades de extensión en la materia, así como aportar un valor agregado adicional: poder formar recursos humanos en procesos de "*vigilancia tecnológica*", actualizados con el estado del arte

Su gestación

La gestación del "*Observatorio Argentino del Ciberespacio*"

(nombre adoptado con posterioridad a su creación) nació a partir de un proyecto de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, dependiente de la Universidad de la Defensa (UNDEF), que posteriormente logró su financiamiento y ampliación en las convocatorias 2017 para proyectos de Investigación UNDEFI.

Si bien el proyecto se presentó a la convocatoria como "*Observatorio de Ciberdefensa*", al poco tiempo de comenzar a trabajar, el equipo llegó a la conclusión de este limitaba los objetivos originales, porque la ciberdefensa, particularmente en Occidente, se encuentra limitada a cuestiones más relacionadas con la protección de infraestructuras críticas. Incluir la ciberseguridad era una opción más integradora, ya que incluiría todos los aspectos relacionados con la Tecnologías de la Información. Pero ninguna la involucraba de manera integral (perspectiva vertical del problema: de la más elevada de las estrategias hasta lo más sencillo del empleo diario o del análisis técnico del problema), e integradora (perspectiva vertical que le permitiera acceder a información útil desde los niveles de decisión hasta de la familia, creando conciencia y cultura). Ello permitiría seguir los principios de trabajo propuestos por la Unión Internacional de Telecomunicaciones (ITU, 2011, pág. 6. 19. 44 y otras).

A partir de estas premisas, y como consecuencia de diversos análisis y evaluaciones, se definió la necesidad de crear un foro de información y conocimiento de la problemática de un nuevo ambiente operacional: el **Ciberespacio**, que se caracteriza por su virtualidad y libertad, según el Manifiesto de John Perry Barlow con la Declaración de Independencia del Ciberespacio (Barlows, 1996).

El ciberespacio permite la integración e integralidad pretendida para el proyecto por su característica de ser un ámbito exclusivo y único del ser humano, que crece y se multiplica a cada instante de la mano de las llamadas **Tecnologías de la Información y las Comunicaciones -**

TIC, que crece a pasos agigantados a través de la movilidad y los teléfonos inteligentes. Se comprendió que el ámbito adecuado y apto de observación era el *ciberespacio*, que ha generado un cambio significativo en los hábitos de la humanidad e impacta de manera radical en todos los ámbitos de la vida. Era el objetivo adecuado de observación y no existía, al menos en nuestro conocimiento, nadie que realizara una tarea de estas características en el ámbito nacional. De allí surgió el nombre de: *Observatorio Argentino del Ciberespacio*.

La meta principal del Observatorio es: ***Difundir y hacer conocer el ciberespacio a la comunidad educativa y a la sociedad en general.***

Definido el objetivo del proyecto, fue necesario establecer cómo llevarlo a cabo. La idea original fue realizar un desarrollo tecnológico basado en Inteligencia artificial que permitiera una búsqueda automática de información relacionada con eventos ciberespaciales, que sería analizada y filtrada por el equipo de trabajo. Las escasas disponibilidades técnicas de la ESGC llevaron al equipo de trabajo hasta la Facultad de Informática de la Universidad Nacional de la Plata, que era la adecuada por sus conocimientos y desarrollos en la materia, y se celebró con ella el convenio correspondiente. Los fondos recibidos del subsidio no eran suficientes para alcanzar este objetivo, por lo que se buscaron otras alternativas.

En una exposición de Vigilancia Tecnológica del Ministerio de Ciencia y Tecnología, (MinCyT), auspiciada por el *Centro de Prospectiva y Tecnología Militar Gral. Mosconi* (CPTM) de la Facultad de Ingeniería del Ejército (FIE), el grupo de trabajo pudo interiorizarse con el Sistema Nacional de Vigilancia e Inteligencia Estratégica que funciona en ese Ministerio y del cual el CPTM administra la *Antena de Defensa y Seguridad.*

Estudiado el tema, se iniciaron todos los procesos para incorporar al OAC formalmente a dicha antena como un observatorio más de la esta. Estos logros se consiguieron después de muchos esfuerzos de las distintas instituciones

participantes y el 2 de julio de 2019 se firmó el acuerdo entre la FIE y la ESGC.

2. La vigilancia tecnológica[1]

Para poder desarrollar sus objetivos, el OAC debió adaptar la modalidad de trabajo para que cumpliera con los estándares establecidos por el MinCyT, para obtener un Observatorio tecnológico[2]. A tal fin, se establecieron los siguientes objetivos:

1. Desarrollo del Programa de Investigación, Extensión y Formación de Recursos Humanos en conjunto con la comunidad educativa universitaria nacional e internacional convocadas por la ESGC (UNDEF).
2. Generar y establecer una estructura multidisciplinaria orientada al análisis y difusión de estudios, informes y reportes sobre el estado, capacidades y evolución de las cuestiones relacionadas con el Ciberespacio.
3. Analizar, desde una perspectiva estratégica y tecnológica, cómo los sistemas fueron vulnerados, cuáles fueron las contramedidas empleadas y cómo fueron las amenazas detectadas.
4. Establecer características y estrategias de captación, reclutamiento, adiestramiento y fidelización de recursos humanos para el área.

---

1 Vigilancia tecnológica es una disciplina propia de la Inteligencia estratégica, cuya tendencia es permitir obtener y recopilar información acerca de desarrollos tecnológicos, patentes y estado del arte en general, que permitan de alguna manera iniciar trabajos prospectivos para la determinación de escenarios futuros y la concepción de modos de acción estratégicos compatibles con los objetivos políticos.

2 Observatorio tecnológico es un elemento intermedio dentro del Sistema de Vigilancia Tecnológica e Inteligencia Estratégica implementado por el MinCyT, que realiza como mínimo acciones de 1) obtener información, 2) analizarla y 3) difundirla y comunicarla. Según la integración de sus recursos humanos y su capacidad, puede también ofrecer servicios de consultoría, prospectiva o incluso inteligencia estratégica.

5. Nutrir el Repositorio Institucional CEFADIGITAL para que estimule el estudio y la investigación sobre temas que abarquen tecnologías cibernéticas, ataques e incidentes cibernéticos, el ciberespacio, la ciberforensia, el recurso humano en el área, entre otros, advirtiendo las nuevas capacidades detectadas en el ambiente ciberespacial.
6. Conformar un grupo de analistas relacionados con el área que permita actuar de forma sinérgica con elementos propios del sistema de ciberdefensa y advirtiendo las nuevas capacidades que se detectan en el ambiente ciberespacial, además de observar el estado del arte en el nivel mundial y su orientación en lo cibernético, como conocer y difundir tácticas y acciones desarrolladas a través del ciberespacio.
7. Colaborar en la extensión del conocimiento del ciberespacio mediante la organización y participación en cursos, seminarios, congresos y como parte de la dirección de trabajos finales y ser jurados en aspectos que se relacionan con el ciberespacio y sus áreas de influencia: ciberdefensa, ciberguerra, cibercrimen, ciberforensia, ciberconfianza, cuestiones estratégicas, legales y doctrinarias, entre otras.
8. Generar informes periódicos acerca del estado del arte en el quinto dominio, desde una perspectiva estratégico-operativa y técnica.
9. Implementar la base de datos para el desarrollo prospectivo en temas de la Defensa Nacional.

Metodología de trabajo

La metodología de trabajo para la Vigilancia Tecnológica en la República Argentina está regida por lo determinado por el MinCyT, y a través de la publicación "*Guía Nacional de Vigilancia e Inteligencia Estratégica*: *buenas prácticas para generar*

sistemas territoriales de gestión de VeIE" (MinCyT, 2015).

El documento fija pautas para la tarea, como la siguiente: "*Para lograr un Sistema Nacional de Ciencia, Tecnología e Innovación (SNCTI) eficaz y competitivo, las empresas, el gobierno y las universidades deben estar informados sobre su entorno, especialmente para identificar aquellos cambios que suponen beneficios o desafíos para sus intereses. En este contexto, las disciplinas de Vigilancia e Inteligencia Estratégica (VeIE) aportan herramientas indispensables para transformar datos en información útil para la toma de decisiones*" (MinCyT, 2015, pág. 9).

Para ser eficaz y competitivo, un sistema de Vigilancia Tecnológica e Inteligencia Estratégica del MinCyT debe tener capacidad de encontrar la información, diseminarla y convertirla en inteligencia útil para asistir a la mejor toma de decisiones.

La vigilancia tecnológica es una actividad de bajo nivel de difusión en las Fuerzas Armadas y el ciberespacio es un nuevo dominio de la actividad militar en pleno auge en el nivel mundial. Es por ello que la implementación de un observatorio para esta actividad resulta oportuna, no sólo para la difusión del estado del arte, sino también para la generación de una base de datos que permita, en el futuro, la realización de trabajos prospectivos. A su vez, es un elemento útil para formar recursos humanos, generar información útil para la toma de decisiones y tratar de incrementar los conocimientos en los claustros y en la sociedad toda.

Actualmente, la Antena Territorial de Seguridad y Defensa recibe aportes de información desde diferentes observatorios, a saber:

Centro de Prospectiva y Tecnología Militar "Gral Mosconi", con sede en la Facultad de Ingeniería del Ejército, dichoCentro es el fundador e iniciador del sistema y quien administra la Antena Territorial de Defensa y Seguridad de la que hablaremos más adelante. (http://www.ceptm.iue.edu.ar/)

El Observatorio Argentino del Ciberespacio, con sede en la Escuela Superior de Guerra Conjunta. (http://www.esgcffaa.edu.ar/esp/oac-boletines.php)

El Observatorio Aeroespacial, con sede en la Escuela Superior de Guerra Aérea. (https://www.esga.mil.ar/Observatorio/boletines.html)

La estrategia que sigue la Antena es poder incorporar en el futuro observatorios de otros ambientes operacionales y del área de seguridad, aspirando como objetivo ulterior convertirse en elementos formales o *ad hoc* para asistir a la toma de decisiones, cuestión que aún no forma parte del consciente colectivo del planeamiento militar.

La forma de trabajo del observatorio se basa en el rastreo permanente del ciberespacio: en fuentes abiertas, en la búsqueda y recopilación de novedades, desarrollos, patentes, noticias, eventos, entre otros.

La actividad es realizada por los denominados *observadores tecnológicos* a través de meta-buscadores, RSS[3] y envíos de noticias de páginas registradas para constituir un cúmulo de información acerca del área de estudio asignada. Los datos obtenidos se guardan en una base de datos (BD) de observadores, disponible para la visualización de los analistas[4].

Los analistas trabajan sobre la información obtenida de cada área, la procesan, corroboran y cruzan con otras e intentan llegar a las fuentes primarias, determinando si se trata de una noticia falsa (*fake news*), para culminar en un proceso de validación que amerite el ingreso a la Base de datos

3 RSS : siglas de Really Simple Syndication Este formato distribuye contenidos sin necesidad de un navegador, utilizando programas llamados agregadores de noticias, diseñados para leer contenidos RSS. Las últimas versiones de los principales navegadores permiten leer los RSS sin necesidad de programas

4 Actualmente este trabajo se realiza de manera manual, por encontrarse la BD en proceso de desarrollo

del Observatorio[5].

Del análisis realizado se seleccionan aquellos elementos que se consideran de interés para los diferentes usuarios y se conviertan en propuestas para el Boletín que periódicamente difunde el observatorio. Algunas veces, por las características y cantidad de información, el analista puede producir un "Reporte"[6].

Otros productos que surgen como consecuencia de la vigilancia tecnológica son los *documentos de interés* (legales, doctrinarios, técnicos operacionales, etc.) que por sus características deben ser accedidos directamente por quienes consultan la página *web* del Observatorio. De acuerdo con las posibilidades y recursos humanos disponibles. Cuando dichos documentos se consideran importantes, son muy voluminosos, complejos o se requiere una interpretación, se puede producir un *informe*[7].

Todos los productos y resultados son enviados a la Antena Territorial de Defensa y seguridad para su difusión. Ello se puede hacer a través de la BD, de los enlaces de las páginas web, en el observatorio o según como lo determine el administrador.

Las áreas de trabajo e interés en las cuales el OAC se encuentra trabajando son las siguientes: 1) **Estrategia**: se ocupa del ciberespacio, un elemento viviente y cambiante donde las tecnologías y los procesos legales y doctrinarios se encuentran en permanente cambio. 2) **Ciberdefensa**: bajo esta área se tratan los aspectos referidos a infraestructuras críticas, sistemas de protección, ataques, conformación de Fuerzas y

5 Ibidem 4

6 Reporte: documento en el cual un analista vuelca su opinión acerca de una o varias informaciones de interés.

7 Informe: documento abreviado en el que el analista explica los contenidos y aspectos relevantes de un *documento de interés.*

desarrollo de recursos humanos. 3) **Ciberseguridad** el objeto de tratamiento está orientado a los problemas relacionados con las TICs y el impacto con la sociedad, organizaciones alertas y evolución relacionadas con el área. 4) **Ciberconfianza**: Esta área surge como puntual recomendación de la ITU y bajo el concepto de integrar una cultura del ciberespacio. Aquí se tratan cuestiones relacionadas con la internet de las cosas (ioT), el impacto de las nuevas tecnologías y como las maneja la sociedad de la información. 5) **Ciberdelito**, **Cibercrimen** y **Ciberguerra**: son áreas variables según cómo fluya la problemática del ciberespacio; tienen una fuerte relación con la ciberseguridad y la ciberdefensa, pero con ciertas características particulares que le dan entidad propia. 6) **Tecnología**: aquí, fundamentalmente, se ha seguido los desarrollos de alto impacto en el ciberespacio, como la inteligencia artificial, la computación cuántica y la robótica, entre otras, y por último, 7) **Ciberforensia**: es un área dedicada a presentar informes técnicos sobre distintos eventos de cualquiera de las áreas de tratamiento.

Todas las áreas de trabajo se orientan principalmente a la información a la comunidad educativa de la UNDEF, a especialistas en Ciberdefensa, a diferentes organizaciones relacionadas con el ciberespacio, universidades y centros de pensamiento con interés en el tema. Asimismo, toda persona que tenga interés en recibir este tipo de información, puede acceder a ella en la página *web* http://www.esgcffaa.edu.ar/esp/oac-boletines.php.

3. Difusión de la cultura del ciberespacio

Bajo este título, se presentan los diferentes esfuerzos realizados en ese período de observación del ciberespacio. Durante ese plazo, se ha ido cumpliendo con los diferentes objetivos y líneas de investigación que se fijaron para el proyecto, que son presentados como:

- El contacto con la comunidad

- Las tareas de extensión
- Cursos dictados y previstos

a) El contacto con la comunidad

El contacto con la comunidad, objetivo de este proyecto, se desarrolló a través de publicaciones periódicas, que denominamos boletines, y la página *web* de la ESGC, que constituye por el momento el sitio oficial del Observatorio.

Los boletines

A lo largo de estos 660 días de observación del ciberespacio, se han realizado 23 boletines. La tarea se ha llevado a cabo mensualmente, a excepción de los meses de enero-febrero, en que se ejecutó de manera bimestral.

El sistema de difusión se realiza a través de una base de datos registrada en la herramienta de marketing digital mailchimp (https://mailchimp.com/), por el momento en forma gratuita, en tanto los suscriptores no superen los 1000. Por la cantidad de requerimientos, probablemente se deba desdoblar la cuenta o pasar a una cuenta arancelada. El correo electrónico empleado para el de registro de la cuenta es observatorioargentinodelciberespacio@conjunta.undef.edu.ar .

Otra modalidad de difusión de los boletines es la denominada *de boca en boca*, y también se hace a través de la publicación que realizan otros centros y observatorios. Esta forma de llegada a nuevos usuarios no tiene un seguimiento estadístico, hasta tanto el potencial usuario no se suscriba al Boletín a través de la página *web*.

Por el momento, los boletines son guardados en el Repositorio Digital del Centro Educativo de las Fuerzas Armadas, CEFADigital (http://www.cefadigital.edu.ar/). Como se verá más adelante, se prevé la construcción de una Base de datos específica para el trabajo y seguimiento de la Información que en el futuro permita una mayor facilidad

para la realización de trabajos de prospectiva.

Las estadísticas que proporciona el sistema de difusión son periódicas en relación con los envíos y con una cantidad de aspectos para su análisis. A los efectos del presente trabajo, se ha realizado una tabla de resumen que, de alguna manera, sintetiza los aspectos de mayor consideración para evaluar la tarea realizada.

TABLA 1

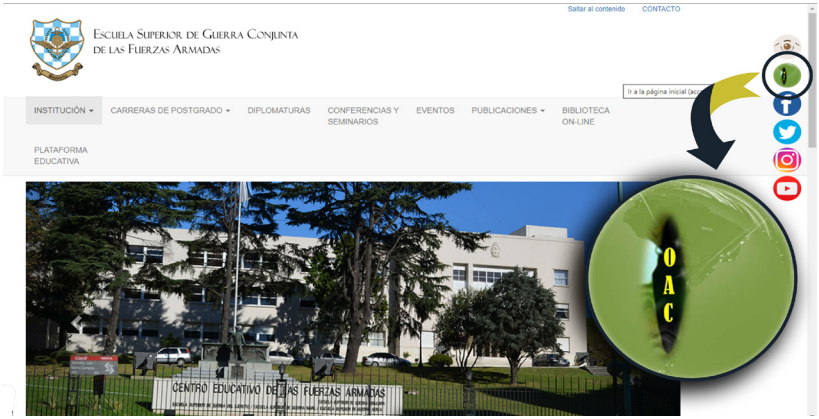
Estadística de Boletines OAC. Elaboración propia con datos de MailChimp.

N°	Actividad realizada	Cantidad	
1	Entregas	14.971	
2	Aperturas	9786	
3	Países y porcentajes	Alemania	0,061
		Argentina	47,87
		Bélgica	0,01
		Brasil	1,16
		Canadá	0,05
		Chile	0,14
		China	0,01
		Chipre	0,05
		Colombia	0,1
		Cuba	0,03
		Ecuador	0,05
		EE. UU.	45,54
		España	0,48
		Francia	0,1
		Guyana	0,03
		Italia	0,11
		México	2,49
		Nicaragua	0,01
		Países Bajos	0,16
		Panamá	0,08
		Perú	0,34
		Rep. Dominicana	0,01
		Singapur	0,01
		Sudáfrica	0,01
		Suiza	0,01
		U.K. (Reino Unido)	0,5
		Uruguay	0,56
		Venezuela	0,03
TOTAL			100

La página *web*

La página *web* del observatorio es un micrositio dentro de la página *web* de la ESGC (http://www.esgcffaa.edu.ar/esp/index.php). En su parte superior derecha, se encuentra el logo del observatorio (figura 1) que permite el acceso (figura 2)

FIGURA 1

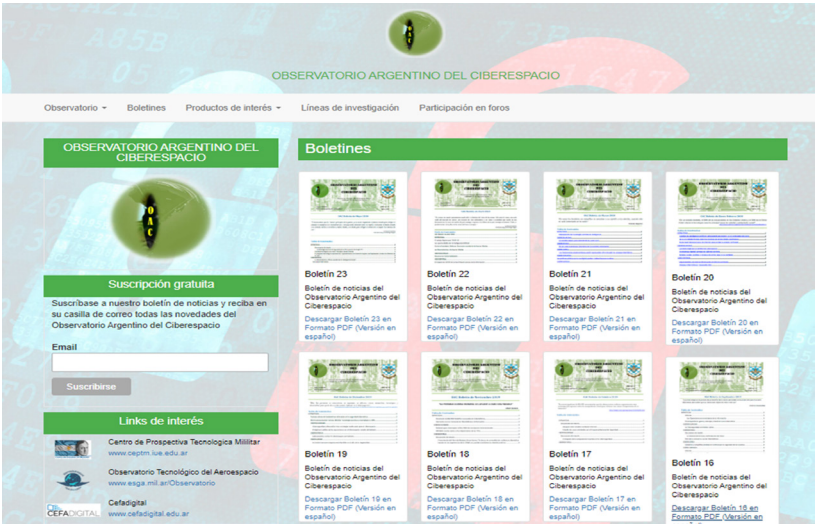


Una vez dentro del micrositio del OAC, se pueden encontrar la totalidad de los boletines emitidos de manera sincrónica, así como otros documentos de interés:

- **Boletines**: el sistema abre por defecto en esta opción. En ella, se pueden ver los boletines, los enlaces a otros observatorios o asociados o el CEFA digital y brinda la posibilidad de registrarse para recibir información.
- **Productos de interés**: son documentos que han sido revisados y/o producidos por analistas del observatorio, que por sus contenidos se aprecian de consulta para quien accede al sitio.
- **Observatorio:** allí hay información general acerca del proyecto, objetivos, miembros, organización y acuerdos alcanzados.

- **Líneas de investigación:** son las vigentes del proyecto.
- **Participación en foros;** presenta algunas de las actividades de extensión del OAC.

FIGURA 3



b) La tarea de extensión

Uno de los objetivos de llevar la cultura del ciberespacio a diferentes ámbitos de la comunidad se cumple a través de tareas de extensión, mediante la participación en foros o conferencias, la realización de cursos, presentaciones en distintos tipos de medios (canales de *streaming*, medios gráficos y seminarios o dando clases en otros ámbitos).

Dichas acciones buscan generar una cultura nacional que permita el conocimiento del ciberespacio, sus aplicaciones, amenazas y desarrollos, de modo tal que la sociedad —en ámbitos específicos, académicos y en general— pueda comprender su importancia para la Nación, la defensa y protección de los intereses nacionales y de la sociedad en general.

WICC 2018

El OAC participó en el Workshop de Investigadores en Ciencias de la Computación (WICC 2018), evento organizado desde 1999 por la Red de Universidades Nacionales con Carreras de Informática (RedUNCI), cuyo propósito es generar un foro para el intercambio de ideas entre investigadores en Ciencias de la Computación para fomentar la vinculación y potenciar el desarrollo coordinado de actividades de investigación, desarrollo e innovación entre ellos. En 2018, el evento fue organizado por la Universidad Nacional del Nordeste y la Red de Universidades con Carreras de Informática, RedUNCI.

El tema presentado fue: *Protección de activos vinculados con la información: preparación para la Ciberdefensa*, y puede consultarse en el Libro de Actas del XX Workshop de Investigadores en Ciencias de la Computación. ISBN 978-987-3619-27-4. Pág. 1021 a 1025. Abril de 2018. Corrientes, Argentina. http://wicc2018.unne.edu.ar/wicc2018librodeactas.pdf, página 1048.

La evaluación, realizada por pares internacionales, mereció una calificación global de 10 (diez) puntos, con un conocimiento del tema por el evaluador de 9 (nueve). Recibió comentarios como: "[es un] *trabajo de sumo interés para el WICC pues plantea diversas líneas vinculadas con la Ciberdefensa y la Ciberseguridad nacional sumando los esfuerzos de expertos en el tema*".

El OAC en canales de streaming

Una de las actividades de difusión más efectivas fue la participación del OAC en un canal de *streaming*, el canal 22 "Islas Malvinas". Esta modalidad de trabajo fue empleada en dos oportunidades.

La primera fue en abril de 2018, donde se presentó la temática *La guerra futura*. En esa ocasión, se trataron las perspectivas del empleo del aeroespacio y sus connotaciones con el espectro electromagnético.

La segunda fue en octubre de 2019, cuando se presentó un informe acerca del ciberespacio como un nuevo ambiente para el desarrollo de la actividad humana. Allí se habló sobre los peligros y posibilidades de este nuevo ambiente, las connotaciones, las relaciones con la inteligencia artificial, la computación cuántica y los posibles escenarios futuros.

Exponiendo ideas en diferentes foros

Se plantean bajo este título los eventos más significativos, sin considerarse los propios de la tarea cotidiana del observatorio y las exposiciones en el marco interno del trabajo académico.

En abril de 2018, se participó en el Workshop Ciberseguridad Ciberamenazas & Delitos Informáticos, organizado por el Foro de Profesionales en Seguridad. En esa oportunidad, el OAC se expuso acerca del *Espectro electromagnético y su relación con el*

ciberespacio, y trató la problemática que conlleva el salto de la tecnología analógica a los desafíos del espectro digitalizado.

En junio de 2018, la UNDEF, a través de la Secretaría de Ciencia y Tecnología, realizó las primeras Jornadas Tecnológicas de la Universidad de la Defensa Nacional. En dicha ocasión, el OAC participó con una exposición sobre la actividad y evolución del Observatorio y los inconvenientes en su desarrollo. Para ello, se presentó un poster relacionado con el evento.

En octubre de 2019, el OAC fue invitado a participar en un ciclo de jornadas internacionales, organizado desde España por Organización DarFe (http://www.darfe.es/joomla/), especializada en tecnologías de la información y comunicaciones.

La invitación fue para exponer en el *Ciclo sobre Ciberdefensa Webinar 3 (nivel estratégico/directivo)*. El tema desarrollado por el observatorio fue *La Estrategia en el dominio ciberespacial*. Se trató la problemática del desarrollo tecnológico y la dificultad de la sociedad, en particular de las personas para adaptarse al nuevo paradigma cultural, social y protocolar que plantea el ciberespacio.

Posteriormente, ya dentro del período de cuarentena, el observatorio tuvo la oportunidad de interactuar con la Maestría de Ciberseguridad y Ciberdefensa de la Universidad Nacional de Buenos Aires (UBA). En dicha oportunidad se disertó sobre *El ciberespacio. Pensando el conflicto futuro*. Allí, se dio una apreciación general sobre el futuro a partir del dilema y compromiso que traerá el concepto de "singularidad" y la formulación de los procesos culturales y educativos actuales,

En busca del estado del arte

La actividad de capacitación del OAC se realiza de manera presencial y en relación con la disponibilidad de fondos para la asistencia a cursos y seminarios. Su objetivo es mantener a los que desarrollan la actividad de analistas y observadores

tecnológicos en el estado del arte, ya que es una materia que muta y progresa a una velocidad a veces difícil de alcanzar.

La situación particular que se vive en razón de la cuarentena, causada por la pandemia del virus COVID-19, ha permitido una mayor disponibilidad de tiempo para acceder a expositores y organizaciones en el plano nacional e internacional de sumo interés. Entre las actividades realizadas, se pueden citar las siguientes:

1. SEGURINFO edición argentina, de abril de 2019 (presencial) y la de edición 4.0, de abril de 2020 vía WEBINAR

2. Seminario de Ciberseguridad (Gestión de la Entidad Digital), agosto de 2019 (presencial)

3. Proyecto AURORA: Webinar Ciberseguridad) entre abril y mayo de 2020, se realizaron;

- Webinar: Reportes de Pentest y Vulerability Assessment
- Webinar: Criptomonedas y Blockchain
- Webinar: Creación de un SOC y CSIRT
- Webinar: Implementación del CyberSecurity Framework NIST utilizando ISO 27001
- Webinar: Implementación de Malware Information Sharing Platform (MISP)

c) **Cursos dictados y previstos**

Dentro de lo que se podría describir como las diferentes formas de ejercitar la extensión académica, está sin duda la docencia regular, que ocupa el nivel más distinguido. El OAC incursionó en esta actividad, por requerimiento de la Dirección de la ESGC, para presentar un curso sobre las cuestiones del ciberespacio para la comunidad en general.

El curso fue preparado, desarrollado y ejecutado bajo la supervisión del OAC, con la concurrencia de prestigiosos profesores de diferentes ámbitos universitarios. Se dictó durante el segundo semestre de 2019, con una duración de 40 (cuarenta) horas reloj, que incluyeron clases, conferencias magistrales y ejercitaciones.

El curso se denominó Programa Intensivo de Introducción a la Ciberdefensa y ciberseguridad, y su objetivo fue "Constituirse en una introducción general a la ciberdefensa y la ciberseguridad mostrando que las mismas requieren enfoques interdisciplinarios y multidisciplinarios, destacando que la ciberdefensa y ciberseguridad, ambas requieren de profesionales con las formaciones de grado más diversas". Sus objetivos específicos fueron los siguientes:

1. Presentar los aspectos generales de ciberdefensa y ciberseguridad, y su relación con la tecnología de la información.

2. Introducir los aspectos generales de ciberterrorismo, ciberespionaje, activismo hacker, cibercrimen y ciberconflictos entre Estados y naciones.

3. Presentar, en forma general, las contramedidas posibles frente al ciberterrorismo, ciberespionaje, activismo hacker, ciberguerra y cibercrimen

4. Destacar la importancia extrema de la ética en los equipos que actúan enfrentando al ciberterrorismo, al ciberespionaje, al activismo hacker y que actúan en episodios ciberbélicos y que enfrenten cibercrimen.

5. estudiar los aspectos jurídicos a ser tenidos en cuenta por quienes actúen enfrentando al ciberterrorismo, al ciberespionaje, al activismo hacker, que actúen en episodios ciberbélicos y que enfrenten cibercrimen.

6. Preparar a los participantes para formar parte de los denominados equipos CERT (*Computer Emergency Response Team*) y para su desempeño en posiciones de liderazgo

en diversos tipos de emprendimientos en el campo de la ciberdefensa y de la ciberseguridad.

Para el presente año, y sobre la base de la experiencia acumulada y los requerimientos que surgieron de la comunidad en el segundo semestre, se ha propuesto la realización de una diplomatura en Gestión de la Ciberdefensa, cuyos programas han sido presentados a la UNDEF para su aprobación. La formación prevé la ejecución de 90 (noventa) horas reloj de clase y entre sus objetivos están:

1. Presentar los aspectos generales de la ciberdefensa y la ciberseguridad, y su relación con la tecnología de la información.

2. Introducir los aspectos generales de ciberterrorismo, ciberespionaje, activismo hacker, cibercrimen y ciberconflictos entre Estados y naciones

3. Analizar los Principios y Sistemas de Gestión más relevantes de la ciberdefensa.

4. Adquirir los conceptos y desarrollar habilidades en el ámbito del Planeamiento Estratégico de la Ciberdefensa.

5. Adquirir habilidades de gerenciamiento y de instrumentación en el contexto de la formación y el entrenamiento de los recursos humanos en ciberdefensa.

6. Analizar los aspectos más sensitivos del Gerenciamiento de la Ciberdefensa de la Infraestructura Crítica.

7. Entender la complejidad del gerenciamiento innovador para enfrentar los nuevos desafíos cibernéticos.

8. Aportar al desarrollo de capacidades, conocimientos, técnicas, procedimientos y aptitudes profesionales para dirigir e integrar equipos técnicos de investigación en ámbitos de la inteligencia aplicada, la defensa nacional y escenarios de toma de decisiones en el Gerenciamiento de la Ciberdisuasión, en los ámbitos estatales y privados.

9. Analizar la importancia del Estándar ISO/IEC 27000 en un contexto de ciberdefensa.

4. Lecciones aprendidas de la observación del ciberespacio

> *En esta área de operaciones, nuestra Fuerza de Tarea se dio cuenta rápidamente que, si bien podríamos ganar cualquier enfrentamiento cinético, estábamos, desde el comienzo mal preparados para llevar a cabo las operaciones de información con la misma capacidad.*
>
> Leonardo J. Flor, *Ejército* (Flor, 2010)

¿Son 660 días mucho o poco tiempo para aprender sobre el ciberespacio? Aprender del ciberespacio, como de la vida, es una tarea permanente donde se absorben conocimientos y se conceptualizan enseñanzas. Todo ello dependerá también de la base de partida que se posea. La realidad es que en este período el Observatorio, a través de sus diferentes áreas de trabajo, pudo establecer algunos conceptos de lo que se puede denominar la estrategia en el dominio ciberespacial.

Si bien los ambientes estratégicos[8] donde operan los sistemas de fuerzas, cualesquiera sean, son influidos por la tecnología, el cibernético se caracteriza por ser completamente virtual. Ello hace que dependa de dos aspectos básicos: la tecnología para acceder y actuar en él y la presencia humana, ya que sólo la atención puede darle vida a una invención abstracta.

La tecnología es un factor común en todos los ambientes

8 Los ambientes estratégicos comenzaron con la historia de la humanidad. La tierra y el agua (primordiales en la guerra), luego se fueron adicionando el aire y el espacio, concebido como aeroespacio (actualmente, cada uno recuperó su propia importancia por las características del conflicto), y finalmente el ciberespacio. No se cierra aquí la cuenta, en la medida en que existen nuevos ambientes mediante los cuales el esfuerzo humano pueda competir para el dominio de la voluntad de otros. En demanda del cumplimiento de objetivos propios, podrán surgir nuevos ambientes.

estratégicos, pero para el caso del aire, el espacio y el ciberespacio es esencial, debido a que poseen características comunes: la intangibilidad, las grandes distancias, la impunidad relativa, los límites basados en tecnologías, la posibilidad de producir efectos, pero no cumplir objetivos estables. Los recursos humanos deben ser adaptados al medio, ya que se distingue una absoluta polaridad entre lo civil y militar, pues en ellos conviven el conflicto y no conflicto.

Se definirá como ambientes estratégicos aquellos en que las acciones de las Fuerzas de un actor puedan ser empleadas en alcanzar los objetivos que se ha impuesto. Aquí aparecen cuestiones que resultarían, a primera vista, poco convencionales. No se habla de Estados-nación sino de actores por un lado, y por otro las acciones de las Fuerzas, que no son necesariamente militares.

Esta disquisición aparentemente ingenua no lo es, porque apunta al hecho de que los conceptos de la guerra erigidos por Clausewitz, el Barón de Jomini, Beaufre, Mahan, Warden y otros muchos teóricos de la estrategia y la guerra se están agotando. Todos ellos sostuvieron que empleo de la fuerza era el elemento decisivo para lograr quebrar la voluntad del enemigo, objeto y naturaleza propia de la guerra.

Existen nuevas formas de ver el conflicto que amplían el campo de acción, y el ciberespacio permite ampliar los efectos de estas nuevas modalidades, así como la teoría de los Coroneles chinos Qiao Liang y Wang Xiangsui, en su libro la Guerra Irrestricta (Xiangsui, 1999), las teorías sobre la Guerra no lineal del general Ruso Valery Gerasimov (Gerasimov, 2014), cuestiones que terminan avaladas por las fuerzas occidentales en libros como Perceptions are Reality (Loudon & Vertuli, 2018) o el manual de la OTAN sobre las operaciones de información rusas (Giles, 2016).

Si bien la naturaleza de la guerra no se ha alterado[9], las

9 La naturaleza de la guerra consiste en imponer la voluntad propia sobre el contendiente.

formas de la guerra se van adecuando. También el concepto de poder ha adquirido nuevos tintes: algunas tendencias no consideran más poderoso a quien tiene más fuerza, sino a quien logra que se cumplan sus objetivos voluntariamente por parte del otro. En esta visión del poder, el uso de la fuerza resulta en una pérdida de poder. El ciberespacio, empleando *inteligencia artificial*, *Big Data* y *computación cuántica*, posee una gran ventaja para moldear el pensamiento, las preferencias y, finalmente, la voluntad.

Ello no significa el fin de las Fuerzas Armadas ni muchos menos sino que, por el contrario, refuerzan la razón de su existencia: la resolución del *problema militar* que surge como consecuencia de la orden política de alcanzar un fin u objetivo mediante el empleo de la defensa nacional.

Cuando el centro de gravedad del problema es intangible, la solución es compleja y no lineal. Deberá darse prioridad a los modos de guerra de la información, de la acción psicológica, el apoyo psicosocial y el empleo de las armas de modo quirúrgico y complementario, para que la sinergia de los efectos combinados permita doblegar la voluntad del adversario.

Como se ha descripto hasta aquí, podría decirse en conclusión que el mayor poder se demuestra cuando lo que quiere quien conduce es lo que hacen los conducidos por su voluntad. Bajo este paradigma el uso de la violencia es una pérdida de poder. Su contraparte, el sometimiento por la fuerza, puede ser más rápido o sencillo y se puede alcanzar por el empleo de la fuerza cinética, pero sólo asegura un éxito militar temporal, que difícilmente logra cerrar el conflicto. Entonces, no cumple con la naturaleza de la guerra, que es quebrar la voluntad del enemigo.

Es por ello que ante el problema militar a resolver, es esencial tener en cuenta cuál es la duración política pretendida del efecto deseado. Este es un factor determinante para elegir una u otra modalidad: si lo que se busca es explotar un recurso

u obtener un beneficio de corto plazo, la fuerza es suficiente; si lo que se busca es algo más perdurable, entonces las Fuerzas aparentemente blandas son realmente las más fuertes.

La influencia de la tecnología en el ciberespacio puede ser apreciada en etapas concretas: a principios de la década de 1980 los componentes que podían identificarse en una oficina eran numerosos (fax, teléfono, agendas, archivos, máquina fotográfica, filmadora, fotocopiadora, computadora, e incluso persistían algunas máquinas de escribir entre otras cosas). La incorporación del celular dotó a la oficina de cierta movilidad. La evolución de los celulares puso la comunicación telefónica en desventaja y se han reemplazado –con muchas ventajas– las oficinas de los años 80 del siglo pasado. Hoy, podría afirmarse que esas oficinas caben en un teléfono inteligente de bolsillo.

El futuro próximo, de la mano de la IA, el Big data, la computación cuántica y la robótica, llegarán a la vida cotidiana de la mano de la llamada "Singularidad"[10]. Esto implica que un equipo de cómputos, robots, etc., podrían ser capaces de superarse de manera recursiva, es decir cuando las máquinas alcancen la misma capacidad o superior a la de la persona humana.

Realidad vs. virtualidad: proporcionalidad en la relación tiempo-espacio.

Hasta nacido el siglo XXI, podría afirmarse que lo real era lo preponderante. En la actualidad, no se puede asegurar que las cosas se mantengan así mientras el tiempo-espacio se va modificando. Esta relación del mundo virtual va ganando cada vez más preponderancia e influencia frente a la realidad. Cada día es más difícil determinar qué es cierto y qué no lo es.

10 Singularidad: desde la perspectiva tecnológica, es el proceso de autoaprendizaje de la inteligencia artificial por el cual esta será capaz de superar los límites del conocimiento racional humano.

Ello posee una implicancia trascendente al tratar el tema del conflicto futuro, que desde la perspectiva del ciberespacio se dará en tres ámbitos: el real, el virtual y el de la información.

El *real* es el mundo donde se produce el enfrentamiento cinético. El *virtual* es donde se pelean la ciberseguridad y la ciberdefensa (abarca desde la seguridad informática básica del individuo en su hogar hasta la defensa de las infraestructuras críticas). El de la *información* tiene por campo de batalla el cerebro de las personas, donde la capacidad excepcional de procesamiento de la inteligencia artificial permite tratar a cada ser humano como único e irrepetible. Se trata, primero, de ganar su simpatía y finalmente su voluntad.

Uno de los graves problemas que enfrenta nuestro modo de ver la civilización es que Occidente puso su foco en el ciberespacio para las cuestiones relativas a la ciberdefensa y la ciberseguridad, olvidando que es sólo la cuarta parte del mundo. Las otras tres partes involucran su acción de lleno en el empleo de la información. La pandemia ha sido una clara demostración de los países orientales en el empleo del control y manejo de la población (Giordano, 2006).

La cuestión del ciberespacio desde la perspectiva de la Seguridad y la Defensa incorpora una pluralidad de conocimientos que las vuelven completamente interdisciplinarias y complejas, donde los recursos humanos militares tradicionales no siempre participan de manera directa. Probablemente, este ambiente requiere de características muy diferentes en sus miembros para los niveles táctico, operacional y estratégico. A modo de ejemplo, debería pensarse que el mejor guerrero en el campo táctico ciberespacial podría ser minusválido, es decir de movilidad corporal reducida.

Como se dijo *ut supra*, en la nueva modalidad de guerra, el campo principal de combate es el cerebro humano, en él combatirán de manera sinérgica por el control de la voluntad del individuo: las acciones duras (ciberdefensa y

ciberseguridad) y las blandas (manejo de la información o desinformación). Ver Tabla 2.

TABLA 2

Elaboración propia, basada en datos del Foro Económico Mundial. https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications

Las acciones duras	Las Acciones Blandas
Estrategias ciberespaciales duras buscan golpear en las Infraestructuras críticas, por ejemplo:	Estrategias ciberespaciales blandas buscan capturar la mente de la sociedad, por ejemplo:
• Fraude electoral. • Comunicaciones y TICs • Cadena de suministro y transporte. • Banca y mercado de Capitales. • Seguridad nuclear • Provocar derrames intencionados de petróleo. • Toma del control de un proceso de fabricación. • Ciudades y urbanización. • Aviación • Corte de energía, etc.	• Convulsionar redes sociales • Identidad digital • Gobernanza y Corrupción, • Generar fake news • Viajes y Turismo • Ransomware • Desconfianza en las IoT • Ataques de colapso en la redes • Desinformación e incertidumbre
Usados de manera coordinada, efectiva y direccionados estratégicamente, junto a otros elementos del poder constituyen un factor coadyuvante de importancia para controlar la voluntad de la sociedad. Crear el mito de que el poder ciberespacial lo logra por sí mismo, es un error como lo fue en la II GM, creer que el poder aéreo era la forma de doblegar el pueblo inglés primero y el alemán después, sólo trajo terrible destrucción y pocos éxitos	

5. **Conclusiones**

La única forma de combate exitoso contra la guerra de la información es crear una cultura del ciberespacio. No se puede vivir en un ambiente desconocido. Antiguamente, cuando las dimensiones eran tangibles, podían identificarse los riesgos con la afección de la vida misma. En la actualidad, el ciberespacio no permite identificar ni entender cuál es su verdadero alcance y el daño que mediante su accionar

se puede provocar. Esta cultura debería percibirse como vinculada férreamente a principios morales, éticos y sociales asociados a la supervivencia de las personas y la sociedad.

La *singularidad* plantea el gran conflicto del futuro próximo (año 2050). La racionalidad[11], esa cualidad de la capacidad humana para el trabajo, será obsoleta. Para triunfar en esa batalla, es importante poseer una diferencia esencial. Es necesario cambiar el sistema de aprendizaje, desarrollar nuevas capacidades cerebrales, para que luego la singularidad sea el gobierno de la inteligencia artificial. Debemos educar y crear sistemas de aprendizaje que permitan estar por encima de las máquinas.

Finalmente, no entender que el campo de batalla del siglo XXI es la mente de las personas, que no existe seguridad interior ni exterior, ni distinción entre militares y civiles, es autocondenarse como sociedad.

La primera línea de combate es el hombre común. La respuesta estratégica es el enjambre social como un todo inteligente. El cibersoldado es un concepto multidisciplinario, de técnicos y profesionales de diferentes áreas y estrategias. El siglo XXI mutará el paradigma de infantería, reina de las batallas, hacia algo como "Los reyes de la guerra serán los cibersoldados dominadores de las mentes de la sociedad".

Los próximos pasos en la observación del ciberespacio

El proyecto continúa generando información mensual para los usuarios, aportando datos a la Antena Tecnológica de Seguridad y Defensa. Se espera que en transcurso de 2 a 3 años se haya generado la suficiente información como para

11 El sistema de aprendizaje humano no ha cambiado desde el siglo V a.C. La escuela socrática definió al hombre como animal racional, y la civilización occidental ha desarrollado preferentemente estas capacidades en detrimento de muchas otras, que aún son pasivas en el cerebro humano y que recién se comienzan a vislumbrar con las neurociencias.

poder establecer un primer salto hacia un proceso de análisis prospectivo en la temática ciberespacio y lograr un sistema de vigilancia tecnológica propio, basado en inteligencia artificial.

El desafío de la mejora continua en esta área es complejo y requiere de esfuerzos permanentes de todos los integrantes del sistema. Se espera en el futuro próximo integrarse con otras instituciones en la materia y desarrollar un mayor número de reportes e informes.

La búsqueda de la excelencia apunta a constituir un centro de referencia para informaciones e investigaciones relacionadas con la ciberseguridad, la ciberdefensa, el cibercrimen, el ciberterrorismo y la ciberforensia, ya sea como órgano de consulta o de asesoramiento en la materia.

Se busca desarrollar acuerdos y convenios con instituciones relacionadas a esta temática, como el que estamos encarando con la Maestría en Ciberdefensa de la UBA, y en el futuro incorporar a diferentes institutos militares y civiles de distintos niveles educativos. Esto, de alguna manera, describe el camino que el OAC intenta con el objetivo de que nuestra sociedad crezca en el conocimiento del ciberespacio.

Continuaremos intentando encontrar satisfacer el grado de interés de la comunidad educativa en principio, y de la sociedad en general, sobre de la necesidad de conocer y saber qué es el ciberespacio y cómo la actividad humana se va adaptando cada día más a este nuevo ambiente.

El OAC es un proyecto de investigación de características diferente a los tradicionales, ya que es interactivo con los posibles usuarios, lo que evidencia un desafío en sí mismo, porque no lleva consigo los estándares habituales de la investigación tradicional.

Asimismo, apunta al conocimiento desde una perspectiva pluralista, donde la hipótesis no es adquirir un nuevo conocimiento, sino transmitir conocimiento a la comunidad educativa y la sociedad toda acerca de un nuevo ambiente de

desenvolvimiento del quehacer humano.

Los resultados de la investigación son la base de desarrollo de una futura potencialidad para ejercer la prospectiva como método de evaluación estratégica en el ambiente futuro de incertidumbre, que permita a los decisores en materias relacionadas con él contar con bases firmes y objetivas en la toma de decisiones.

Referencias bibliográficas

Barlows, J. P. (8 de febrero de 1996). *https://nomadasyrebeldes.files.wordpress.com.* Recuperado el 23 de Mayo de 2018, de Manifiesto de John Perry Barlow (español) Declaración de independenciadelciberespacio:https://nomadasyrebeldes.files.wordpress.com/2012/05/manifiesto_de_john_perry_barlow-1.pdf

Flor, L. J. (31 de octubre de 2010). *https://www.armyupress.army.mil.* Obtenido de Cómo aprovechar la energía potencial de las Operaciones de Información: https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20101031_art007SPA.pdf

Gerasimov, V. (6 de julio de 2014). *https://inmoscowsshadows.wordpress.com.* Obtenido de The 'Gerasimov Doctrine' and Russian Non-Linear War: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Giles, K. (2016). *Handbook of russian information warfare.* Roma, Italia: NATO Defense College "NDC Fellowship Monograph Series". doi:http://www.ndc.nato.int

Giordano, E. (17 de noviembre de 2006). Obtenido de El 'laberinto' tecnológico y las nuevas formas de contro social: https://core.ac.uk/download/pdf/51385117.pdf

ITU. (enero de 2011). *https://www.itu.int.* Obtenido de La búsqueda de la Paz en el Ciberespacio: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-S.pdf

Loudon, & Vertuli. (2018). *Perceptios are reality* (This book is part of The US Army Large-Scale ed.). Fort Leavenworth, Kansas: Army University Press.

MinCyT. (2015). *https://www.argentina.gob.ar.* Obtenido de Guía Nacional de Vigilancia e Inteligencia Estratégica: https://

www.argentina.gob.ar/sites/default/files/lib_ins_guia-nacional-de-vigilancia-e-inteligencia-estrategica-veie.pdf

Ministerio de Ciencia y Tecnología. (2015). *http://www.mincyt.gob.ar.* (M. d. Tecnología, Ed.) Recuperado el 23 de Mayo de 2018, de http://www.mincyt.gob.ar/adjuntos/archivos/000/043/0000043043.pdf

Xiangsui, Q. L. (1999). *Un restrictied Warfare.* (Beijing: PLA Literature and Arts Publishing House.

Palabras clave: *Ciberespacio – observatorio – proyecto – lecciones aprendidas*

Key Words: *Cyberspace - observatory - project - lessons learned*

Abstract

This article shows a synthesis of the activity carried out by the Observatorio Argentino del Ciberespacio (OAC), since its creation, during 2 years of continuous activity of observation new virtual environment for mankind. The cyberspace shows an exponential growth in the number of people who access it, as well as the time they dedicate to it.

Until not long ago, cyberspace was the object of limited use to communicate and perform certain specific tasks, today almost every real world activity is carried out in it, from social and work relationships to the appearance of virtual sports, entertainment, research and study. The pandemic put it in the center of the stage for all human activities, whether they there are personal, family, educational and/or social.

This article goes beyond its aim to show the evolution of the OAC and also tries to focus in the interaction and articulation with the society and the environment, to comment on the lessons learned and the strategies observed by those who work in it, to analyze the impact of the technologies and, finally, to give guidelines for its sustainability.