CIBEROPERACIONES

Héctor Gómez Arriagada*

La información es una herramienta útil para la toma de decisiones y tiene una significativa gravitación en los resultados; por lo que es imprescindible contar con sistemas o componentes que aseguren el acceso a la calidad y veracidad de ésta, con el propósito de tomar las acciones ofensivas o defensivas que permitan obtener una ventaja.

Las Operaciones de Información tienen el propósito de afectar el ciclo de toma de decisiones del adversario y proteger el propio, por medio de acciones desarrolladas en diferentes dominios. Las ejecutadas en el dominio físico buscan atacar o defender la infraestructura física asociada al Mando y Control y la toma de decisiones, siendo objetivos típicos las redes de comunicaciones, los sensores, medios de búsqueda y los propios Mandos, entre otras; y que son susceptibles de ser afectados por medios kinéticos tradicionales. En el dominio cognitivo se ejecutan operaciones destinadas a afectar la percepción por parte de los tomadores de decisiones, siendo el instrumento típico para ello las operaciones psicológicas, aunque también pueden considerarse como parte de las mismas el engaño o la decepción militar.

Existe además un tercer dominio en el que se ejecutan Operaciones de Información, el que para mejor comprensión y ajuste al presente artículo se denominará como ciberespacio, aunque en la doctrina de Guerra de Información normalmente se le conoce como dominio informativo, de data o de información. Éste es un dominio intangible y artificial que surge de la convergencia tecnológica de redes para el transporte de datos, las tecnologías para el procesamiento de los mismos y los sistemas para la representación del significado de dichos datos.

Pero el ciberespacio no es tan solo interconexiones, sino que además interrelaciones e interacciones

personales, similares a las que se realizan en el mundo físico, pero a un volumen, cobertura y velocidad tales que se perciben como instantáneas, masivas y globales. En definitiva es un medioambiente que surge de la convergencia de la infraestructura de las TIC[1], en el que se producen interacciones humanas o automáticas, que ofrece recursos para acceder o generar contenido informativo en múltiples formatos y en el cual pueden desarrollarse actividades virtuales que se manifiestan con efectos en el mundo físico.

En lo avanzado de este siglo, ya no hay espacio para el escepticismo respecto del impacto del ciberespacio en las actividades humanas, así como

* Capitán de Fragata. Oficial de Estado Mayor. Magíster en Informática y Doctorado en Comunicación. Destacado colaborador de la Revita de Marina, desde 2008
1. TIC: Tecnologías de la información y comunicaciones.

de su potencial para generar efectos en el mundo real. La crítica dependencia de las tecnologías de la información y el sinnúmero de interacciones a través del ciberespacio que personas y organizaciones realizan como parte de su rutina diaria, dan cuenta de ello. Del mismo modo sería un error señalar que la actividad militar está ajena a lo anterior, ya que es una realidad en la conducción militar actual la tendencia de disponer de mecanismos que permitan, por un lado, mantener constantes flujos de datos desde sensores o medios de búsqueda, para disponer de panoramas operacionales actualizados permanentemente mientras que, por otro, se ha transformado en un imperativo el contar con enlaces ininterrumpidos para difundir órdenes y obtener retroalimentación a lo largo de toda la cadena de Mando.

Esto último sugiere entonces que en atención a la criticidad e importancia para sostener estas funciones, resulta imprescindible que las organizaciones militares ejerzan el control por el tiempo necesario, de aquella porción del ciberespacio que resulta relevante para sostener sus operaciones; para lo cual deberán identificar las amenazas que puedan impedírselo, tomar las medidas para enfrentarlas y reducir las vulnerabilidades que faciliten su materialización. Simultáneamente esta situación ofrece la oportunidad para desarrollar acciones ofensivas para, precisamente, negar el empleo del ciberespacio a un adversario por medio de la explotación de sus propias vulnerabilidades.

Es decir, al igual que en la tierra, el mar, el aire o el espacio exterior; en el ciberespacio también es posible la manifestación de actividades que sirven a los propósitos militares y, al igual que en las demás dimensiones de la guerra, en él pueden desarrollarse operaciones de una naturaleza ad-hoc tendientes a asegurar su empleo o bien para negárselo al adversario.

Las ciberoperaciones militares.

Las ciberoperaciones deberían entenderse como un instrumento más para la solución de problemas militares en su amplio espectro y por lo mismo, implican eventualmente enfrentar a un antagonista. Pueden, por tanto, ser defensivas cuando buscan detectar, neutralizar y mitigar el impacto de un ataque; o bien, ser ofensivas cuando se utilizan para obtener inteligencia a través del ciberespacio o para negar su empleo. Es decir, las ciberoperaciones implican intencionalidad, voluntades contrapuestas y el enfrentamiento en el ciberespacio con fines militares, elementos claves que permiten distinguir las ciberoperaciones de otras actividades como la seguridad informática o las operaciones de información.

En la Doctrina Conjunta de Operaciones de Información de EE.UU. del año 2006 (DOD, 2006)[2], las ciberoperaciones son llamadas *Computer Network Operations* (CNO), pero en otros países son también conocidas como Guerra Informática, Ciberguerra, Guerra Cibernética o Guerra de Redes. En la doctrina señalada se clasifican en las *Computer Network Defense* (CND), *Computer Network Atack* (CNA) y las *Computer Network Exploitation* (CNE). Las CNE y las CNA buscan sortear las medidas de seguridad de la infraestructura de información crítica del adversario o enemigo, ya sea para obtener inteligencia en base a la extracción de informaciones o el monitoreo de sus actividades, las primeras; o bien, para degradar o neutralizar dicha infraestructura, las segundas. Para ambos tipos de ciberoperaciones se requiere una planificación operacional acuciosa y el empleo por parte de especialistas de los procedimientos, técnicas y herramientas[3] que forman parte del arsenal de armas para operar militarmente en el ciberespacio.

2. La Doctrina Conjunta de Operaciones de Información fue reeditada el 27 de noviembre del año 2012. En la nueva edición se hace referencia general a las Cyberspace Operations, de las cuales también existe una publicación conjunta que describe su doctrina. Sin embargo, los conceptos señalados se siguen empleando en las FF.AA. de EE.UU. como pude observarse en AF (2011; p.41) y en AWC (2011, p.7).
3. Conocidas coloquialmente como de hacking o craking.

Las CND por su parte, hacen un uso intensivo de sensores de vigilancia para detectar y neutralizar tempranamente los intentos de ataque sobre la infraestructura de información crítica propia. Forman parte de un dispositivo defensivo en profundidad que deben complementarse con medidas de seguridad informática preventivas o de barrer; así como también, con acciones preplaneadas para reaccionar a los ataques y minimizar el impacto de los mismos.

Operación de seguridad informática preventivas o de barrera.

La efectividad tanto de las ciberoperaciones defensivas como de las ofensivas o de explotación, dependen críticamente de contar con una adecuada Inteligencia respecto de las capacidades del adversario para operar en el ciberespacio, de lograr superiores capacidades operacionales, de capital humano competente, entrenado y confiable; de capacidad de investigación y desarrollo, y de contar con el adecuado sostenimiento logístico y financiero.

Experiencias mundiales.

La experiencia extranjera en la implementación y ejecución de las ciberoperaciones es heterogénea. En EE.UU., por ejemplo, se han conformado Cibercomandos en distintos niveles de conducción, partiendo desde el estratégico con el *U.S. Cybercommand*, organismo que centraliza las operaciones militares en el ciberespacio para negar su empleo al adversario, sincronizar la defensa de las redes del Departamento de Defensa y asegurar su empleo en apoyo a las operaciones militares (DOD, 2010). Cada rama de las FF.AA. cuenta a su vez con un Cibercomando, con los que contribuyen sinérgicamente a los propósitos del *U.S. Cybercommand*.

En el caso de la *U.S. Navy*, el *U.S. Fleet Cyber Command* ejecuta operaciones en el ciberespacio tal como han sido descritas hasta aquí, pero considera además dar apoyo a las operaciones navales por medio del control y operación de las redes de comunicaciones, la inteligencia de señales, operaciones de información, guerra electrónica y capacidades espaciales; es decir, ha combinado en un solo comando el control de las operaciones de información, las comunicaciones, las ciberoperaciones, las operaciones espaciales y algunas funciones de la Inteligencia (DON, 2012).

De manera similar el *U.S. Army Cyber Command* señala que se ha concentrado en la operación, mantenimiento y defensa de las redes del Ejército estadounidense así como en las operaciones de redes; aun cuando bajo su Mando se encuentran subordinados el Comando de Operaciones de Información (donde se concentran las CNO), el Comando responsable de defender y mantener las redes de comunicaciones del Ejército y el Comando de Inteligencia y Seguridad (Army, 2013). Por su parte, la Fuerza Aérea de EE.UU. agrupa dichas tareas en la *24th Air Force Wing 67* de Guerra de Redes, responsable de organizar, entrenar y equipar fuerzas para ejecutar CNO; el Ala 689 de Comunicaciones de Combate, dedicada a proveer a las fuerzas expedicionarias comunicaciones y control de tráfico aéreo entre otras; mientras que el Ala 688 es la responsable de las Operaciones de Información (AF, 2013).

La doctrina de Operaciones de Información del Ministerio de Defensa del Reino Unido, considera las CNO como parte integral de las mismas y las subclasifica del mismo modo (MOD, 2002). Su Estrategia Marítima considera que las ciberoperaciones van más allá de los sistemas

de información, señalando que las funciones de Mando y Control, Inteligencia, Vigilancia y Reconocimiento pueden ser susceptibles a un ataque cibernético, que afecten el proceso de toma de decisiones (MOD1, 2011 p.3-22). Por su parte, su Doctrina Aérea y Espacial considera las CNO como aquellas Operaciones de Información destinadas a lograr efectos deseados a través del "espacio de batalla digital" (AS, 2009). En la Doctrina de Operaciones del ejército en tanto, las CNO son denominadas *Computer Network Actions*, centradas en el ciberespacio y subclasificadas de la misma manera ya descrita (BA, 2010).

La Estrategia de Ciber Seguridad del Reino Unido, por otro lado, establece como responsables de la Ciber Seguridad Nacional al GCHQ[4] y al Ministerio de Defensa, ambos con la misión de "detectar y derrotar" las ciber amenazas (CO, 2011). Para lo anterior durante el año 2012 se creó en el Ministerio de Defensa el *Defence Cyber Operations Group* (DCOG), una Ciber Unidad Conjunta (*Joint Cyber Unit*) asentada en el GCHQ[5]; el *Global Operations and Security Control Centre* y otra Ciber Unidad Conjunta para reaccionar en contra de las amenazas a la seguridad de la información (CO, 2011).

En Brasil, el 21 de diciembre del año 2012 el Ministerio de Defensa promulga su *Política Cibernética de Defesa*, con la finalidad de orientar las actividades de la defensa cibernética en el nivel estratégico, y de guerra cibernética en los niveles operacional y táctico (MDB, 2012). Dentro de sus objetivos señala que espera asegurar de manera conjunta la preparación y empleo operacional del ciberespacio (*espaço cibernético*) por parte de las FF.AA., impedir o dificultar su utilización en contra de los intereses de la Defensa Nacional, colaborar con la obtención de inteligencia desde fuentes cibernéticas y cooperar a la movilización militar para asegurar capacidades operacionales y de disuasión (MDB, 2012)[6]. La organización de la ciberdefensa de Brasil consideró la creación del Sistema Militar de Defensa Cibernética (SMDC), siendo su órgano principal el Centro de Defensa Cibernética (CDCiber), bajo responsabilidad del Ejército[7].

En el caso de China, desde que ésta inició su proceso de modernización de sus FF.AA., con énfasis en la informatización (*informationization*) y la creación de una estructura interconectada de coordinación para las operaciones terrestres, aéreas, marítimas, espaciales y del espectro electromagnético; ha establecido una doctrina que sostiene que en las etapas iniciales o previo a un conflicto, se requieren asegurar los flujos y el dominio de la información en el espacio de batalla, mientras se lo niega al adversario con un uso coordinado de acciones de guerra electrónica, ataques kinéticos y CNO (Krekel, 2009); estrategia identificada como *integrated network electronic warfare o wangdian yitizhan* (OSD, 2011). China emplearía el ciberespacio en apoyo a las operaciones militares para atacar redes logísticas, comerciales y de comunicaciones, para obtención de inteligencia y como un factor multiplicador de la fuerza en combinación con ataques kinéticos; agregando que su concepto de las CNO comprende, al igual que la doctrina occidental, las CNA, CND y CNE (OSD, 2011).

Conclusiones.

Se considera el Ciberespacio como el medioambiente artificial compuesto por los computadores y las redes que los interconectan para el transporte, procesamiento, almacenamiento y representación de datos o información en múltiples formatos; así como por las interrelaciones e interacciones entre personas o máquinas que estas tecnologías permiten de manera global, masiva e instantánea y que tienen manifestación en el mundo físico.

Como es probable que en la actualidad las FF.AA. tengan un alto grado de dependencia de su infraestructura de información para sostener sus actividades operativas o administrativas, es que surge la oportunidad de ejecutar acciones

4. Government Communications Headquarters: Agencia de Inteligencia del Reino Unido responsable de monitorear o interferir emisiones electromagnéticas, acústicas o de cualquier otro tipo, así como dar soporte en idiomas y criptografía; a las FF.AA., al Gobierno o cualquier organización especificada por el Primer Ministro (IS, 1994).
5. Con el rol de desarrollar tácticas, técnicas y planificación para operar y asegurar el libre empleo del ciberespacio.
6. El actual Comandante del CDCiber, el General José Carlos do Santos, señala que si bien la política del Ministerio de Defensa de Brasil prioriza la Defensa Cibernética, también se preparan para operaciones militares de guerra cibernética y para la Inteligencia (De Sá, 2012).
7. Aunque, según se ha señalado, a futuro probablemente terminará constituyendo un servicio integrado por todas las FF.AA.

en el ciberespacio para negar o restringir su empleo por parte de un potencial adversario afectando sus operaciones, así como la necesidad de defenderlo para asegurar los procesos propios que dependen de él. Es por ello que muchos países han reconocido el potencial de operar militarmente en el ciberespacio y la naturaleza específica de esta dimensión, con la creación de Comandos con la misión de desarrollar la capacidad, planificar y ejecutar ciberoperaciones defensivas y ofensivas.

Se ha convertido el ciberespacio, entonces, en una dimensión más del espacio de batalla contemporáneo, transversal a la terrestre, marítima, aérea o espacial; siendo evidente que las operaciones de esta naturaleza serán nuevos instrumentos que emplearán las FF.AA., del mismo modo como en su momento sucedió con innovaciones como la artillería, la aviación de combate, los submarinos, las comunicaciones inalámbricas o la guerra electrónica, entre otras.

Las ciberoperaciones no son una cuestión técnica, ni administrativa, ni logística; son un asunto operativo. Las defensivas dan protección a sistemas y procedimientos vitales para las operaciones propias, mientras que las ofensivas contribuyen concretamente a degradar las capacidades enemigas. En ambos casos, actúan sobre potenciales centros de gravedad.

* * *

BIBLIOGRAFÍA

1. *AF. (2013). 67th Network Warfare Wing, Mission. Web site, disponible en enero del 2013 en http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15330*
2. *AS. (2009). AP 3000, British air and space power Doctrine. Air Staff, Ministry of Defence, Fourth Edition. Disponible en enero del 2013 en http://www.raf.mod.uk/rafcms/mediafiles/9E435312_5056_A318_A88F14CF6F4FC6CE.pdf*
3. *Army. (2013). U.S. Army Cyber Command; organization. Web site, disponible en enero del 2013 en http://www.arcyber.army.mil/org-arcyber.html*
4. *AWC. (2011). Information Operations Primer. U.S. Army War College Dept. of Military Strategy, Planning, and Operations & Center for Strategic Leadership. Noviembre. Disponible en enero del 2013 en http://www.carlisle.army.mil/usawc/dmspo/Publications/Information%20Operations%20Primer%20AY12%20Web%20Version.pdf*
5. *BA. (2010). Army Doctrine Publication, Operations. Development, Concepts and Doctrine Centre, Ministry of Defence. Disponible en enero del 2013 en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33695/ADPOperationsDec10.pdf.*
6. *CO. (2011). The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world. Cabinet Office, Noviembre; London. Disponible en enero del 2013 en www.cabinetoffice.gov.uk*

7. *De Sá, Nelson. (2012). CDCiber – Entrevista com o General José Carlos dos Santos. DefesaNet, cobertura especial, 8 de mayo. Disponible en enero del 2013 en http://www.defesanet.com.br/cyberwar/noticia/5953/CDCiber-%E2%80%93-Entrevista-com-o-General--Jose-Carlos-dos-Santos*
8. *DOD. (2006). Joint Publication 3-13; Information Operations. Departamento de Defensa de EE.UU. Washington. Disponible en enero del 2013 en http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf*
9. *DOD. (2010). United States Cyber Command Fact Sheet. US Department of Defense Office of Public Affairs. Disponible en enero del 2013 en http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf*
10. *DON. (2012). OPNAV instruction 5450.345: Mission, functions, and tasks of Commander, U.S. Fleet Cyber Command and Commander, U.S. Tenth Fleet. Department of the Navy, Office of the Chief of Naval Operations. Washington. Disponible en enero del 2013 en http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-400%20Organization%20and%20Functional%20Support%20Services/5450.3-45.pdf*
11. *IS. (1994). Intelligence Services Act 1994. The Intelligence and Security Committee web site. Disponible en enero del 2013 en http://isc.independent.gov.uk/reference-material*
12. *MDB. (2012). Política Cibernética de Defesa. Ministerio de Defensa de Brasil, Primera Edición. Disponible en enero del 2013 en www.defesanet.com.br/cyberwar/noticia/9128/MD---Politica-Cibernetica-de-Defesa*
13. *MOD. (2002). Joint warfare publication 3-80, Information Operations. Chiefs of Staff, Joint Doctrine and Concepts. Disponible en enero del 2013 en http://ics-www.leeds.ac.uk/papers/pmt/exhibits/2270/jwp3_80.pdf*
14. *MOD1. (2011). Joint Doctrine Publication 0-10, British Maritime Doctrine. Chiefs of Staff, Joint Doctrine and Concepts. Disponible en enero 2013 en https://www.gov.uk/government/publications/jdp-0-10-british-maritime-doctrine*
15. *Krekel, Bryan. (2009). Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Prepared for The US-China Economic and Security Review Commission; Northrop Grumman Corporation, Octubre. Disponible en enero del 2013 en http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf*
16. *OSD. (2011). Annual report to Congress; Military Power of the People's Republic of China. Office of the Secretary of Defense, Mayo. Disponible en enero de 2013 en http://www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf*