Las Operaciones de Información, Disuasión y Uso de la Fuerza*

Roger W. Barnett

Roger Barnett es profesor de estudios de guerra naval en la Escuela de Guerra Naval, donde enseña cursos selectivos sobre guerra de la información y control de armas. Asimismo, sirve como profesor adjunto en la Universidad Salve Regina y en la Universidad Southwest Missouri State. Se retiró de la Marina en 1984, habiendo servido en cruceros, destructores y en los comandos del Cuartel General en Washington. Obtuvo su Bachillerato de la Universidad Brown, y su Maestría y Doctorado de la Universidad de Southern California.

"Hace un par de años atrás, nadie tomaba seriamente la guerra de la información. Pero mientras más aprendía uno sobre ella, uno se interesaba más". Pensamiento típico que tienen muchos hoy en día acerca de la guerra de la información. Dicha frase implica la ecuación: *ignorancia = complacencia.* Pero incluso la guerra de la información ha estado allí desde al menos el siglo V A.C. Dicha guerra también se presentó poderosamente en la Segunda Guerra Mundial -se trataba de una clave para la victoria en los teatros europeos y del Pacífico- y desempeñó un papel importante en la Guerra del Golfo de 1991. ¿Entonces, por qué muchas personas piensan que los Estados Unidos (especialmente las fuerzas militares de los EE.UU.) no está familiarizado con la Guerra de la Información? Y ¿por qué existe tal preocupación sobre "tomarlo con seriedad"?

Quizá se trata de elevar dicho interés en lo referente a las nuevas vulnerabilidades para la guerra de la información que se han venido exponiendo en los últimos años, en la medida que las sociedades y las economías se volvieron más dependientes del flujo libre y rápido de la información. En los Estados Unidos, tanto la Oficina de Conta-

* Del *Naval War College Review,* Primavera 1998, Volumen LI, Número 2, Secuencia 362.

bilidad General y la Junta de Ciencia para la Defensa han presentado reportes detallados sobre el tema. Dichos reportes reconocen la existencia de problemas que deben resolverse, pero ninguno puede calificarse como un llamado para tomar una acción urgente. Sin embargo, el Jurado todavía está fuera; la Comisión del Presidente sobre la Protección Crítica en Infraestructura se encuentra actualmente en sesión, estudiando ocho infraestructuras domésticas críticas

Para las fuerzas militares de EE.UU., los temas de interés central en las operaciones de información se concentran en dos: disuasión y empleo. La Disuasión del ataque de la información contra los Estados Unidos y sus amigos y aliados, y el uso de las operaciones de información en los asuntos de Estado constituyen el centro dual de la atención.

El presente artículo examina la disuasión en la medida que se relaciona con las operaciones de información y luego ofrece algunos análisis de su empleo. Argumenta primero que para los dos tipos de disuasión -general e inmediata (o dirigida)- los Estados Unidos posee fortalezas inherentes, pero también puntos débiles identificables que pueden rectificarse. Segundo, el presente artículo señala que existen argumentos importantes y válidos contra la permisión de las operaciones de información que pueden caracterizarse como "usos de la fuerza" en el Derecho Internacional. Las "operaciones de información" más rutinarias pueden entenderse como operaciones "antiterroristas", como actos de defensa propia que no incluyen "el uso de la fuerza", mientras sea así, mayor será su contribución a la seguridad nacional de los Estados Unidos.

Operaciones de Información

Como un instrumento del arte de gobernar, las operaciones de información pueden emplearse en el soporte de la política nacional de igual manera que la diplomacia y la política económica. Disponible en tiempos de paz, crisis, y en todos los niveles de la guerra, las operaciones de información tienen aspectos ofensivos y defensivos. A diferencia de las acciones económicas para sancionar las actividades de otros Estados -medidas que generalmente se consideran actos graduales y lentos-, las operaciones de información pueden imponer rápidamente un daño severo con niveles bajos de violencia. Esta es una de las mayores características que ubican a las operaciones de información en un rubro diferente al de los otros instrumentos del arte de gobernar.

También existen otras diferencias. Primero, el ambiente de la información cambia rápidamente. Una operación que tendría éxito actualmente podría fracasar mañana -o en una hora- debido a que se ha alterado la configuración de la computadora, un canal de comunicación, una red, o un protocolo de software. Tal como en las operaciones encubiertas y clandestinas, los "agentes" ("caballos de Troya" o "trampas") pueden colocarse para una activación posterior. Asimismo, la diferencia ante los medios tradicionales radica en la dificultad de observar y evaluar los resultados de las operaciones de informa-

ción. Un virus podría implantarse en la computadora de un adversario, el atacante no podrá evaluar si el virus es o no efectivo. Por supuesto, una de las técnicas defensivas de las operaciones de información consiste, en realidad, en negar al adversario la habilidad para medir sus resultados, haciendo el problema mucho más dificil. Asimismo, a menudo linda con la imposibilidad de saber si las defensas de uno son o no efectivas. Quizá nuestro sistema está siendo explotado, pero no estamos conscientes de nuestra vulnerabilidad. Si estamos seguros, ¿es porque las defensas trabajan, o porque nadie las está probando? ¿Seguiremos seguros de aquí a diez minutos? La magnitud de dicha falta de conocimiento es grande y contribuye a la preocupación de que *ignorancia = complacencia.*

Dada la importancia de las redes de computadoras modernas, los sistemas de comunicación, y los bancos de datos electrónicos, las operaciones de información deben estar totalmente integradas en una política de seguridad nacional global. En tiempos de paz, pueden contribuir a la prevención del conflicto, o pueden usarse para responder a las crisis y a las hostilidades abiertas. Pueden o no involucrar capacidades o unidades militares. En tiempos de crisis, las operaciones de información pueden emplearse para resolver los desacuerdos, fortificar la disuasión o prepararse para la posibilidad de un conflicto abierto. En la guerra, pueden alcanzar directamente los objetivos estratégicos, operativos y tácticos o asegurar otros medios para lograr tales objetivos. El documento oficial del Estado Mayor "Visión Conjunta 2010" identifica un marcador, afirmando que las operaciones militares en el futuro requerirán la *superioridad* de información, "la capacidad de reunir, procesar y diseminar el flujo ininterrumpido de información mientras se explote o se impida una habilidad del adversario de hacer lo mismo."

Las acciones ofensivas que utilizan las operaciones de información incluyen aquellas que mueven la información de un lugar a otro, la destruyen, promulgan la desinformación y corroen, degradan, interrumpen o niegan los flujos de datos. Las acciones defensivas buscan proteger la información de uno de acciones similares de un adversario. Claramente, pueden usarse una variedad de medios en las operaciones de información ofensivas y defensivas. Éstas incluyen los pilares militares adecuadamente reconocidos del comando y control de la guerra (guerra electrónica, seguridad de operaciones, decepción, operaciones psicológicas y destrucción fisica); otros medios lo constituyen la "guerra de hackers*," la "guerra de información económica," y la "cibergue-rra." En tiempos de paz, un objetivo de seguridad fundamental de los Estados Unidos es evitar la guerra. Si el conflicto se presenta, la meta sería terminarlo rápidamente y con el menor daño posible sin comprometer los intereses vitales o los objetivos mayores. Las operaciones de información pueden desempeñar papeles importantes en la prevención y la persecución exitosa de la guerra. Sus fundamentos de efectividad acerca del papel en la disuasión deben considerarse como un uso de la fuerza.

* Individuos que postulan que la información debe ser libre para todos, por lo cual tratan de ingresar y violar los sistemas de seguridad "firewalls" de las diversas entidades, sean militares o civiles.

La Preparación Estadounidense para la Disuasión de un Ataque de Información

Por mucho tiempo considerada como el producto de la capacidad y el deseo, la disuasión constituye un tema del que se ha hablado mucho pero no se le ha dedicado el tiempo suficiente para pensar. La razón es que la disuasión "general" se basa generalmente en el mantenimiento de la paz. La disuasión *general* proviene del mantenimiento de la capacidad y el deseo de infligir un daño severo como represalia contra aquellos que dañan la paz. Básicamente, mediante el soporte de una fuerza militar grande y altamente capaz los Estados Unidos transfiere su habilidad para castigar a aquellos que atentan contra la paz. La disuasión general no requiere la comunicación de una amenaza especifica contra los agresores; su efectividad depende de la presencia de un arsenal de capacidades tangibles.

Además del castigo, la disuasión general puede trabajar mediante la negación. Está pensado plenamente en aquellos que dañarían a los Estados Unidos, o sus intereses, de modo que no se les permita alcanzar sus objetivos; reconociendo que no puede tener éxito, se les disuade de hacer el intento. Para lograr la disuasión mediante la negación, uno intenta primero realizar actos hostiles lo más dificil posibles de realizar, y luego, si dicho ataque se lleva a cabo, minimizar su logro del propósito del atacante. Este es el enfoque usado por los terroristas, los raptores y los extorsionistas. El mensaje para los perpetradores es: Ustedes no pueden prevalecer, entonces ¿por qué intentarlo?

La disuasión general a través de la amenaza de *castigos* requiere el mantenimiento de una capacidad ofensiva y la proyección creíble del deseo de usarla. La disuasión general mediante la negación requiere las defensas firmes y una historia de negaciones consistentes para vencer las amenazas coercitivas.

La disuasión "dirigida" o "inmediata" opera en niveles diferentes de especificidad. Reconoce que algunas veces la disuasión general no trabaja -una postura sin referencia a un objetivo particular será considerada débil o irrelevante- y que se requiere la *amenaza* o el *aviso* de una disuasión dirigida, inmediata o específica. Por lo tanto, la disuasión dirigida es "más fuerte" que la disuasión general, que representa el esfuerzo explícito de una nación para disuadir a un adversario de llevar a cabo un acto indeseable (o fracasar al realizar un acto deseable). La disuasion general fracasó entre los británicos y los argentinos en el conflicto de las Islas Malvinas en 1982. Los británicos nunca comunicaron claramente a los argentinos que usarían la fuerza para proteger las islas -en efecto, la Oficina Británica de Relaciones Exteriores y el Commonwealth señalaron lo contrario. La disuasión general falló nuevamente en la guerra del Golfo Pérsico en 1990; no se envió ninguna amenaza específica a Saddam Hussein sobre la realización de actos contra Kuwait con la participación de la fuerza militar. En ambos casos, el agresor concluyó que podría descontar una disuasión general. Se necesitó un discurso disuasivo o una defensa poderosa para impedir la agresión. Pero ninguno se realizó.

Al igual que la disuasión general, la disuasión dirigida puede operar me-

diante la amenaza del castigo o mediante la negación. La disuasión inmediata mediante la amenaza del castigo requiere objetivos identificables, y trabaja mejor en grupos organizados que pueden localizarse y atacarse -por ejemplo, los gobiernos. Contra individuos u organizaciones que son menos formales y más difíciles de localizar -hackers o terroristas de computadoras- la disuasión mediante la negación es la forma más apropiada.

La disuasión de cualquier clase o modalidad requiere tanto *la capacidad* como *el deseo.* Desde el fin de la Guerra Fría, los Estados Unidos ha disfrutado de una superioridad militar sobre todos los Estados del mundo. Mantiene su habilidad para usar la fuerza hasta incluir la devastación nuclear de cualquier país u organización localizable. Las operaciones de información, aunque no involucran invariablemente el uso de la fuerza, contribuyen a la capacidad agregada de disuasión de los Estados Unidos. Incuestionablemente, para la disuasión mediante la amenaza de castigo, el factor de la capacidad en la ecuación de los Estados Unidos es virtualmente abundante. Tal como observaremos, *el deseo* de los Estados Unidos en dicha área parece ser deficiente.

Los adversarios que no cuentan con o no temen el castigo deben ser disuadidos mediante la negación. Dicho tipo de disuasión se basa en defensas poderosas, de modo que los agresores no puedan lograr sus objetivos directamente al atacar primero. La defensa contra el ataque de la información requiere una identificación efectiva y mecanismos de autenticación, operadores de sistemas adecuadamente capacitados y disciplinados, firewalls* de gran seguridad, y métodos de auditoría y seguimiento. Para los Estados Unidos, la falta de dichas protecciones constituye puntos débiles que los adversarios podrían explotar con éxito. Debido a que ninguna defensa resulta muy poderosa en su punto más débil, la habilidad de los Estados Unidos y de otras sociedades abiertas para disuadir el ataque de la información mediante una estrategia de negación es, y siempre será, sospechosa.

Sin embargo, se debe entender que la complejidad de los sistemas constituye en sí una barrera ante el ataque. Los sistemas de comunicación (particularmente las redes de comando y control gubernamentales) están diseñadas para ser redundantes y para fracasar agraciadamente (es decir, ofreciendo "modos de bajas" sucesivos) en lugar de catastróficamente. Los métodos alternativos de transporte de la información abundan, y las rutinas complejas de software ayudan a asegurar la confiabilidad y autenticidad de la información transportada. Mientras que la persona de dentro del sistema muy versada en una arquitectura del sistema podría evaluarlo como vulnerable, para un externo, probablemente parecerá un sistema extremadamente robusto y difícil de atacar. Ello ayuda a explicar por qué una gran fracción de ataques exitosos sobre los sistemas de información se originan -o reciben asistencia- desde dentro.

El deseo, al igual que la capacidad,

* Un *firewall* es un medio para evitar otros, que no sean los usuarios autorizados del sistema, penetren a un sistema de información. Los *Firewalls* generalmente requieren cierta clase de clave u otro tipo de identificación.

se extiende a lo largo de la disuasión general y dirigida, y pertenece tanto a la amenaza de castigo y a la negación. Aunque el deseo americano de disuadir mediante la amenaza del castigo generalmente parece robusto, la resolución de la nación de tomar represalias contra un ataque de información es cuestionable; en dicho campo, la preparación para ejercer una disuasión dirigida no ha sido actualmente probada y analizada ampliamente. ¿Los Estados Unidos, reconociendo una amenaza particular de un ataque de información planeado, emitiría un discurso disuasivo específicamente sobre ese punto? En el caso de la negación, los Estados Unidos ha tenido un éxito en la detención de terroristas, extorsionistas políticos y otros que podrían contemplar la conducción de un ataque de informacion para objetivos posteriores.

El deseo se comunica en varios modos, a veces mediante la declaración de la política, a veces mediante la demostración - por el *uso* abierto de la capacidad. Si ninguno de éstos se presenta, entonces la disuasión es general. Es en esta situación que los Estados Unidos se encuentra a sí mismo en las operaciones de información. Posee una gran capacidad para conducir operaciones de información de carácter vengativo; incluso no se han hecho declaraciones sobre qué pasaría si la infraestructura de la información crítica de una nación fuera atacada por agentes hostiles, tampoco se han presentado demostraciones. Al mismo tiempo, sus defensas - instrumental para la disuasión mediante la negación- no son adecuadas. Por ende, hoy, en lo referente a las operaciones de información, los Estados Unidos se basa en una forma más débil, la disuasión general. Pero, incluso en el caso de la disuasión general en las arenas de las operaciones de información, se sospecha que la capacidad americana para negar es la mejor, y su deseo de castigar es incuestionable.

Cuando llega la hora de la disuasión, la capacidad de los Estados Unidos para conducir las operaciones de información con el fin de castigar no constituye un problema. Los problemas para la disuasión surgen cuando uno considera las defensas contra las operaciones de información llevadas a cabo por adversarios, o por el deseo de los Estados Unidos- especialmente en el caso de la disuasión dirigida.

La matriz resume la situación de disuasión actual para las operaciones de información:

Preparación para la Disuasión de las Operaciones de Información

		Disuasión General	Disuasión Dirigida
Capacidad	Castigo	Poderoso	Poderoso
	Negación	Defensas	Defensas
		Sospecha	Sospecha
Deseo	Castigo	Cuestionable	No tratado
	Negación	Poderoso	No tratado

La Disuasión para las Operaciones de Información

La capacidad de los Estados Unidos para conducir las operaciones de información es bastante grande, pero su vulnerabilidad para las operaciones de información de otros es también considerable, debido a que las defensas y el deseo americano de actuar son, o podrían percibirse, adecuadamente, como débiles. En el caso de la disuasión mediante la amenaza de castigo, entonces los fundamentos resultantes en la cuestión del deseo; en cuanto a la disuasión mediante la negación, se trata de una cuestión de defensas adecuadas y de cómo demostrar el deseo suficiente para una disuasión dirigida efectiva. Los problemas para la resolución tienen, por lo tanto, que ver primero con la capacidad de negación, que es centralmente una cuestión de fortalecimiento de las defensas de las operaciones de la información; y segundo, con el deseo de castigar a sus agresores, que necesitan ser asegurados mediante discursos de política y otras acciones que sustenten la disuasión general y dirigida.

De los dos problemas de interés central para la fuerza militar de los Estados Unidos, el segundo, el empleo de las operaciones de información, se relaciona estrechamente con el primero, la disuasión. El empleo puede ser directo o indirecto, pero refuerza la capacidad y el deseo. Su objetivo es desalentar los ataques de información contra los Estados Unidos o sus amigos y aliados o alcanzar los objetivos de seguridad mediante una acción ofensiva.

El uso o la amenaza de la *fuerza* ocupa una posición central en la disuasión, pero la disuasión no se basa solamente en ella. Para que la disuasión sea efectiva, es suficiente que un adversario crea que él quedará en peores condiciones -quizá mucho peor- para llevar a cabo una acción particular en lugar de intentarla.

Muy importante, las operaciones de información han tendido a ser juzgadas por los lineamientos que rigen el uso de la fuerza: la necesidad, la discriminación. la proporcionalidad y la humanidad. Claramente, sin embargo, algunas operaciones de información no incluyen el uso de la fuerza: operaciones psicológicas, muchas aplicaciones de la decepción, y también una variedad de "códigos bombas" de cómputo, virus y "chipping". Además, las operaciones de información pueden conducirse por otras fuerzas militares.

La distinción es importante en la medida que se consideren a las operaciones de información en la misma infraestructura. Tal como la fuerza, su uso será condicionado por cuatro categorías de factores -operativos, organizacionales, legales y morales. Permítasenos examinar cómo dichas categorías podrían aplicarse erróneamente a las operaciones de información, considerando que cada una de ellas restringiría (o restringen) la libertad disponible para las operaciones de información, que afectan el deseo de usar o amenazar su empleo. Los adversarios o los adversarios potenciales reconocen dichas restricciones y el cómo afectan al deseo de los Estados Unidos de actuar o defenderse contra las acciones hostiles. El efecto global de dichas restricciones en la disuasión no está totalmente claro, pero ciertamente no es para fortalecer la disuasión.

Restricciones Operativas. Los estadounidenses que toman las decisiones actualmente observan un código operativo de acuerdo al cual usan la fuerza. Aunque utiliza la fuerza sólo con renuencia, cuando es necesario prefieren aplicarla masivamente con el fin de minimizar las bajas amigas y terminar con las hostilidades tan pronto como sea posible. Para tal fin, los objetivos deben ser claramente definidos de modo que el progreso hacia ellos pueda monitorearse, de modo que sea evidente cuando se hayan alcanzado. Los objetivos deben seleccionarse cuidadosamente. Los no combatientes no deben ser objetivos directamente, y deben preservarse los santuarios religiosos, obras maestras, monumentos, etc. Se debe minimizar el daño colateral. Además las consecuencias no intencionadas deben, en la medida de lo posible, ser regladas. El fratricidio -enfrentamiento "azul con azul"- debe evitarse. En efecto, es deseable que se minimicen las bajas en ambos lados.

Mediante este código, y hablando en general, aunque un ataque preventivo por parte de las fuerzas estadounidenses es deseable y manejable en el nivel táctico de la guerra, resulta problemático en el nivel operativo, e improbable en el nivel estratégico. Es decir, los Estados Unidos va a la guerra sólo cuando se ve forzado hacerlo, pero una vez que lo hace, se enfrenta en actos agresivos, rápidos y decisivos. Debido a esta negación mayor para prevenir en el nivel estratégico, los Estados Unidos es más vulnerable para la sorpresa estratégica y, por lo tanto, a sus efectos no deseables. Incluso, si no se considera que las operaciones de información involucran el uso de la fuerza, la inhibición americana tradicional sobre la iniciación de una acción hostil -especialmente en el nivel estratégico- ya no es pertinente. Además, debido a que las operaciones de información pueden llevarse a cabo a grandes velocidades y sin advertencia, las implicancias de la sorpresa son potencialmente serias en todos los niveles de la guerra. Si se reconoce dicha distinción sobre la aceptabilidad operativa de las operaciones de información, los estadounidenses que toman las decisiones deben evaluar las posibilidades de que un adversario tome represalias y deben determinar si pueden defenderse contra él o tolerar tal represalia. Si no pueden, los Estados Unidos probablemente se verá disuadido de atacar.

Aunque éstos luzcan como un grupo de restricciones operativas sin excepcion, en realidad se trata de un grupo único como un código de lucha. La mayoría de ellas son claramente de menor preocupación para los oponentes estadounidenses potenciales, en relación con sus propios actos. Sin embargo, un acto que *es* de interés para ellos es el último: evaluar el potencial del adversario para tomar represalias. Si la disuasión mediante la amenaza del castigo posee un fundamento, éste es.

Aun así, mediante las restricciones operativas que los Estados Unidos puso sobre sí mismo, el asunto de la represalia se volvió un problema. Es decir, con relación al castigo, la *certeza* de la represalia es lo que disuade. La disuasión se ve debilitada en la medida que un adversario está inseguro en lo que concierne al nivel de represalia o si después de todo ocurrirá. Por supuesto, eso no constituye un problema que se relaciona sólo con la capacidad sino también con el deseo de tomar represa-

lias. Se trata de una tarea especialmente dificil para las operaciones de información: convencer al enemgo potencial de que uno tiene el deseo de tomar represalias con las operaciones de información y de que el atacante saldrá peor debido a la represalia.

En las operaciones de información, tal como en el terrorismo, existe la posibilidad de que un ataque devastador se realice sin que se identifique al perpetrador. La dificultad de determinar la fuente de hackers de cómputo o el origen del virus da pie a la preocupación de atrapar a un culpable o tomar represalias contra un atacante. Incluso si el atacante puede identificarse, surgen interrogantes sobre la forma adecuada de una acción vengativa. Tales interrogantes enervan la disuasión al reducir la certeza de las represalias. Si uno no puede formular una forma apropiada y efectiva de represalia, uno está obligado a depender de la disuasión mediante la negación.

Restricciones Organizacionales. El uso de la fuerza por parte de los Estados Unidos se ve restringido también por el modo de organización del país. Históricamente, las democracias están más propensas a rechazar el uso de la fuerza que otros tipos de gobierno. Si bien es cierto que el Jefe del Estado Mayor es el Presidente, el poder para declarar y apoyar la guerra recae sobre la rama legislativa, colocando así otro nivel de restricción sobre el uso de la fuerza. Si las operaciones de información se consideran como el uso de la fuerza -y especialmente si dichas operaciones son preventivas o de primer uso-, se debe considerar cómo analizar dichos problemas.

De modo similar, muchas formas de libertad y derechos de la privacidad, incluyendo la de información personal, se consideran fundamentales en los Estados Unidos. Éstos tienen gran importancia para la conducción de las operaciones de información, en particular cuando se intenta rastrear o seguir la fuente de ataques sobre la infraestructura de una nación. Las poderosas fuerzas legales y sociales son bastante resistentes al monitoreo gubernamental de, o a la interferencia en, el flujo libre de información, sea plena o encriptada.

Existen otros obstáculos organizacionales. La prensa libre y neutra en los Estados Unidos representa otra fuente de restricciones. El poder de los medios para plantear interrogantes y problemas difíciles tendría que considerarse antes de que se lleven a cabo operaciones de información. Existen las restricciones planteadas por organizaciones externas de las cuales los Estados Unidos es miembro, especialmente las Naciones Unidas y la OTAN. La sola membresía en dichas organizaciones significa la aceptación de niveles adicionales de restricciones. Las coaliciones ad hoc poseen un efecto restrictivo similar

Restricciones Legales. Un órgano significativo de restricciones legales sobre el uso de la fuerza se ha formalizado. Reside en el Derecho Internacional, en particular en el derecho del Conflicto Armado, y en los acuerdos de control de armas, que constituyen documentos legales.

El derecho establece una diferencia entre el inicio del uso de la fuerza *-jus ad bellum-* y cómo se usa la fuerza en la guerra *-jus in bello.* Para satisfacer el derecho que rige al anterior, el uso de la

fuerza debe surgir de una causa que sea justa, sea motivada por las intenciones correctas y sea autorizada por una autoridad competente. Además, se deben pasar cuatro pruebas: el uso de la fuerza debe poseer una oportunidad razonable de éxito, que se espera produzca un balance neto del bueno sobre el villano, y sea un último recurso; finalmente, la paz debe esperarse como resultado. La Carta de las Naciones Unidas da otro paso *jus ad bellum,* solicitando que el uso de la fuerza sea, siempre y exclusivamente, en defensa propia.

Una vez que se ha iniciado la guerra, se hayan o no satisfecho los requisitos *jus ad bellum,* se deben satisfacer criterios diferentes: las estipulaciones *jus in bello* mencionadas anteriormente - necesidad, proporcionalidad, discriminación y humanidad. El derecho del conflicto armado, codificado en las Convenciones de La Haya y Ginebra y en otros documentos legales, ha proporcionado la especificidad a los requisitos *jus in bello.* Éstos tratan con los derechos y las responsabilidades de los países beligerantes y neutrales, y con la protección de los neutrales en tiempos de guerra. Por su parte, el control de armas limita cuantitativa y cualitativamente los inventarios y los despliegues de armamentos. No han existido acuerdos específicos sobre el control de armas dirigidos a limitar las operaciones de información. Sin embarago, en efecto, con su énfasis en las medidas de edificación de la confidencia y la transparencia operativa, el control de armas ha actuado para entorpecer las operaciones de información efectivas.

Otros tratados y acuerdos ejecutivos poseen un efecto potencial sobre las operaciones de información. El Acuerdo sobre la Organización Internacional de Telecomunicaciones vía Satélite (INTELSAT) de 1973, por ejemplo, busca asegurar que los satélites se usen sólo para fines pacíficos. Aunque el acuerdo reconoce los sistemas de satélites con propósitos militares y establece excepciones, el Departamento de la Defensa usa frecuentemente los sistemas civiles. Si las operaciones de información que involucran dichos sistemas (incluyendo, por ejemplo, porciones de Internet) tienen que considerarse siempre como "no pacíficas" es un problema fundamental que no se ha establecido aún.

De igual modo, los actos encubiertos en concordancia con el manto de la seguridad nacional son regidos por el derecho federal. Se requiere un descubrimiento presidencial y la aprobación del congreso. Una variedad de operaciones de información en tiempos de paz podría encontrarse en dicha categoría, especialmente en aquellas que involucran el emplazamiento de los "agentes" de la operación de información, pero esto, tampoco, se ha determinado aún.

Retricciones Morales. Además y por encima de las restricciones operativas, organizacionales y legales, existen las consideraciones morales. La política de relaciones exteriores de los Estados Unidos siempre ha tenido un elemento moral; se pregunta si la nación puede llevar a cabo un acto particular o seguir una determinada línea política que está legalmente permitida y resulta prudencialmente atractiva. Los estadounidenses que toman las decisiones se ven a menudo limitados por los requisitos competentes, por ejemplo, la necesidad

de una intervención humanitaria y el principio de la no interferencia en los asuntos internos de otros Estados. Incluso resulta difícil articular un código moral en dichas circunstancias, así como seguir una de modo consistente.

Entre los problemas más saltantes se encuentra la separación intelectual del uso de la fuerza o las operaciones de información entre las naciones estado en el contexto de las relaciones interpersonales. Las acciones internacionales se juzgan a menudo indiscriminadamente bajo el mismo grupo de reglas y con la misma plantilla moral como en el caso de las situaciones interpersonales. Incluso las acciones que un estado pueda hacer moral y legalmente son muy diferentes de aquéllas que los individuos pueden hacer. Dean Acheson señaló la diferencia hace treinta años atrás: "*Un buen trato de los problemas proviene de la urgencia antropomórfica de considerar a las naciones como individuos... el hecho es que las naciones no son individuos: [por lo tanto,] la causa y el efecto de sus acciones son totalmente diferentes.*"

Los estadounidenses que toman las decisiones creen que resulta importante para la nación actuar como un líder moral en las relaciones interestatales. Una consecuencia de dicha visión es que las políticas o las acciones no deben causar un sufrimiento innecesario en los no combatientes del Estado objetivo. Además, los estadounidenses tienden a sentirse incómodos con la noción de superioridad, creyendo fuertemente en la igualdad. Lo cual, de cierta manera, hace reconocer que los Estados Unidos presenta una disuasión basado en sus capacidades superiores. La justificación pública del uso de las operaciones de información será importante, debido a que los aspectos morales de la política estadounidense lo demandarán. El cómo se justifica moralmente el uso de las operaciones de información irá de la mano hacia la identificación con, o hacia, el divorcio del uso de la fuerza.

Como resultado del entre tiempo de dichos factores, la habilidad de los Estados Unidos para disuadir un ataque de información puede evaluarse como no tan problemática. La capacidad de la nación para responder ante un ataque de información por un Estado o un grupo organizado y localizable no puede ponerse en duda; su deseo de hacerlo así constituye otro problema. Si el atacante es amorfo y trabaja oculto, los Estados Unidos tendrá que depender de la disuasión mediante la negación, excluyendo los daños que un atacante de información competente y determinado pueda buscar causar, o actuando de tal manera que incluso los ataques exitosos prueben ser no beneficiosos para su perpetrador. Desafortunadamente, la auto protección es un aspecto clave de la disuasión mediante la negación, y constituye otro punto débil de las operaciones de información estadounidenses.

La disuasión por castigo y negación serían difundidas mediante la articulación de una política de disuasión y de otras acciones que comunican el deseo de los Estados Unidos de desempeñar un papel activo en las operaciones de información a lo largo de la junta. Tal como la Junta de Ciencia para la Defensa concluyó, "*la disuasión debe incluir una expresión del deseo nacional tal como se encuentra expresado en el derecho, y la conducta, una política declaratoria relativa a las consecuencias de un ataque de la guerra de la información contra los Estados Unidos, y una indicación de la elasticidad de la infraestructura de la información para sobrevivir a un ataque.*"