Armas Cibernéticas: La igualdad de condiciones a nivel internacional

Ross M. Rustici

Este artículo fue originalmente publicado en inglés en la revista Parameters, *otoño de 2011.*

UNA DE LAS mayores preocupaciones que enfrenta Estados Unidos hoy en día, es la de mitigar su vulnerabilidad ante las armas cibernéticas. En los últimos 20 años, las amenazas cibernéticas han pasado de solitarios piratas informáticos (*hackers*) motivados por el dinero y prestigio, al crimen organizado y actores estatales. La complejidad y capacidades de estas amenazas aumentan en directa proporción al nivel de conectividad en la sociedad. A pesar del continuo desarrollo de las amenazas cibernéticas, relativamente poca atención se le presta a analizar cómo estas amenazas tendrán un efecto en la conducción de la guerra y en el sistema internacional. La mayoría de la actual literatura sobre la guerra cibernética, en el mejor de los casos, considera la guerra cibernética como un multiplicador de fuerza. Muchos expertos ignoran sus efectos como un elemento de ataque independiente cuando citan diversas razones desde la respuesta de EUA en relación con los ataques en Pearl Harbor y el 11-S, hasta la incapacidad del bombardeo estratégico en la Segunda Guerra Mundial para doblegar la voluntad de las poblaciones civiles en Inglaterra y Alemania, sin usar las operaciones militares combinadas. Estas perspectivas son correctas al argumentar que las operaciones cibernéticas ofensivas sin el poder tradicional ni convencional serán, en gran medida, inútiles. Sin embargo, esta planteamiento analítico presume que las armas cibernéticas se utilizarán como un ataque ofensivo preventivo. Las capacidades de ataque de largo alcance de la guerra cibernética tienen la capacidad de ser muy eficaces, si se las emplea como un arma anti-coerción. En principio, una fuerte capacidad cibernética es una fuerza de disuasión que mitigará, significativamente, la injerencia externa en los asuntos internos y regionales.

En vista de que no hay ningún caso confirmado de un ataque cibernético en gran escala avalado por un Estado, los analistas actualmente se ven obligados a estudiar distintos sistemas de armas y teorías para ayudar a que tanto los militares como los políticos comprendan cómo se pueden utilizar las armas cibernéticas y cuáles vulnerabilidades crea este nuevo tipo de arma. Dadas las singulares características del ciberespacio y las armas cibernéticas, ninguna tecnología ni teoría actual proporcionará una comprensión adecuada. Sin embargo, cuando se usan los principios tanto de la teoría del poder aéreo estratégico como la de los primeros debates sobre la doctrina y el poder de disuasión de las armas nucleares, las capacidades aproximadas de las armas cibernéticas se tornan mucho más claras.

En el pasado siglo, el concepto del poder aéreo estratégico se convirtió en uno de los principales dogmas de la guerra moderna.[1] Los estrategas comprenden sus limitaciones para ganar una guerra de proporciones existenciales, pero además encontraron su utilidad en los conflictos de corta duración entre dos partes desiguales. La superioridad aérea requerida en una campaña aérea cuesta trillones de dólares y requiere una extensa red de bases en ultramar para ubicar aeródromos y puertos que puedan recibir a los grupos de portaaviones. Este nivel de inversión

El Señor Ross Rustici es analista de investigación contratado que trabajó con el Instituto de Estudios de Seguridad Nacional de la Universidad Nacional de Defensa. Se especializaen las relaciones estratégicas estadounidenses-chinas y el Ejército Popular de Liberación (PLA), incluyendo las operaciones, tamaño de fuerzas y transparencia de defensa de las fuerzas navales del PLA.

va más allá de las capacidades de la mayoría de los Estados. Como consecuencia, las armas cibernéticas tienen el potencial de convertirse en una fuerza equilibradora porque requieren una fracción de la inversión pero pueden llevar a cabo la mayoría de las mismas misiones.

Además, las primeras teorías nucleares se enfrentaron a muchos de los mismos problemas que en la actualidad enfrentamos cuando intentamos comprender las armas cibernéticas. Si bien Estados Unidos y la Unión Soviética, finalmente llegaron a la misma conclusión sobre cuál es el verdadero uso de las armas nucleares en la guerra, se tardaron dos décadas para hacerlo. Aunque las armas cibernéticas puedan resultar ser suficientemente asombrosas para crear una nueva manera de destrucción mutua asegurada (*MAD*, por sus siglas en inglés)[2], es mucho más probable que los pensamientos iniciales en cuanto a que las modestas demostraciones de prueba y defensa de ensamblaje pasarán a ser una represalia masiva mucho más reveladora.

Así como la revolución industrial dio lugar a cambios fundamentales en la conducción de la guerra, la era de la información está llevando a una nueva y económica opción para la defensa estratégica. Las capacidades de la guerra cibernética actualmente pueden desempeñar la mayoría de las tareas estratégicas que antes requerían la supremacía aérea. Según los analistas estadounidenses, todo, desde el sistema de salud hasta la red eléctrica, constituye un blanco cibernético viable.[3] Un breve vistazo a los blancos de las recientes campañas aéreas de EUA demuestra cuán frecuentemente se seleccionan blancos en la infraestructura civil en una campaña de bombardeo estratégico. En el mundo interconectado de hoy en día, tanto la infraestructura civil como las instalaciones militares son cada vez más vulnerables a la perturbación cibernética.[4] En consecuencia, el futuro de la conducción de la guerra y los límites impuestos sobre la coerción internacional básicamente tiene la capacidad de cambiar.

En el presente artículo se examinará cómo las armas cibernéticas presentan nuevos riesgos a las sociedades conectadas a la red y se explorará el efecto específico que pueden tener en Estados Unidos, así como también las implicaciones de estas nuevas capacidades cibernéticas. Además, se concluye el mismo con una breve discusión sobre las posibles limitaciones y problemas relacionados con el uso de las armas cibernéticas como una manera de disuación. El objetivo del artículo no es ser definitivo o sugerir opciones políticas específicas; más bien es un primer paso hacia el pensamiento sobre el uso de las armas cibernéticas en la política de defensa de otras naciones y sus ramificaciones en la libertad de acción de Estados Unidos.

Amenazas cibernéticas emergentes

A fin de comprender las verdaderas posibilidades que tienen estas armas, primero se debe definir la diferencia que existe entre la Explotación de Redes de Computadoras (*CNE*, por sus siglas en inglés) y el Ataque contra Redes de Computadoras (*CNA*, por sus siglas en inglés). El *CNA* es el acto de discontinuidad, negación, degradación o destrucción (las 4D, por sus siglas en inglés) de las redes de computadoras, la información contenida en la red o los sistemas que controla. La *CNE* en realidad es una actividad de recolección de datos de inteligencia. Si bien un actor que intenta una *CNE*, de vez en cuando, comete un error que resulta en una de las 4D, los casos de un *CNA* deliberado son sumamente escasos. Aunque Estados Unidos y el resto del mundo sufren ataques de *CNE* en la escala de millones de intentos diarios, hasta el momento solo han habido unos pocos aparentes casos significativos de un *CNA*. Si bien, casi a diario se entablan violentas guerras entre *hackers*, la destrucción de sitios cibernéticos apenas califica como un *CNA* en el nivel de violencia declarado por un Estado. Los países como Estonia, Georgia e Irán, proporcionan los ejemplos más conocidos de *CNA* significativos y, tal vez, son los únicos casos auspiciados por un Estado. Debido a la escasez de verdaderos estudios de caso, los encargados de escribir sobre el tema del *CNA* se ven forzados a considerarlo que es técnicamente factible y llevar a cabo presunciones a partir de esa primicia. Si bien, la cantidad de casos reportados de una *CNE* exponencialmente aumenta cuando los blancos son cada vez más suceptibles y el nivel de explotación es inigualado, las capacidades de llevar a cabo un *CNA* a nivel mundial son, en su mayor parte, desconocidas y no probadas.

Extrapolando las capacidades de la *CNE* y considerando cuán poca información concreta hay sobre el *CNA* y las armas cibernéticas, sabemos que los actores que poseen tecnología avanzada pueden desactivar las redes de energía eléctrica, paralizar los sistemas ferroviarios, distorsionar la bolsa de valores, averiar los sistemas de purificación de agua y las plantas de tratamiento de aguas residuales, abrir las compuertas de represas y paralizar las operaciones de refinerías de petróleo.[5] En una sociedad tan interconectada como Estados Unidos o Europa, la mayoría, por no decir toda la infraestructura civil, es vulnerable a los ataques cibernéticos. En vista de la velocidad y precisión con el que se puede llevar a cabo un ataque cibernético, se pueden emplear estas armas para cualquier cosa, desde un tiro de advertencia para un adversario durante una crisis, hasta un ataque catastrófico que podría costarle al Estado trillones de dólares e incontables vidas. Esta amplia gama de usos hace singulares a las armas cibernéticas; además, el hecho de que un arsenal de armas cibernéticas es considerablemente económico, significa que la capacidad destructiva disponible para los Estados pobres o débiles no tiene precedentes. La habilidad de rápidamente atacar, sin aviso y en una gran escala, las hacen excepcionalmente aterradoras. Una campaña cibernética bien perpetrada, junto con cuidadosas relaciones públicas, tiene el potencial de traumatizar a una sociedad de maneras que no se han visto desde Nagasaki.[6] Si bien las armas cibernéticas no crean el mismo espectacular efecto visual que produce un mísil nuclear o, incluso, convencional, las formas como son usadas las hacen una herramienta intrínseca de la guerra psicológica. A diferencia de las armas convencionales o hasta nucleares, no hay previo aviso de un ciberataque del exterior. La incapacidad que tiene una sociedad de fortalecerse ante un ataque inesperado aumenta la efectividad de las armas cibernéticas. No saber cuál será el siguiente ataque o cuándo ocurrirá, tiene un profundo efecto en la víctima y hace que las armas cibernéticas sean singulares entre todos los posibles sistemas coercitivos.

Dicho esto, un ataque cibernético tipo "Pearl Harbor" no tiene sentido para la mayoría del mundo. A pesar de estas evidentes vulnerabilidades, sin las capacidades convencionales para explotar una población confusa y desorganizada, los ciberataques probablemente provocarán que la población civil apoye al gobierno, en lugar de la capitulación. Lo que sucedió en Estonia y Georgia ejemplarizan este fenómeno. En Estonia, la comunidad de *hackers* rusos paralizaron los medios de comunicación afiliados, ciertas funciones bancarias y sitios cibernéticos por varios días como represalia por la decisión del Gobierno estonio de sacar de Tallinn un monumento en honor a las Fuerzas Armadas soviéticas. Sin embargo, en vista de que no hubo intervención militar correspondiente que sacara ventaja de los efectos de la campaña cibernética, los efectos, en gran parte, fueron financieros y de corto plazo.[7] El Estado no regresó el monumento a su lugar original y, como resultado de los ataques, Estonia presumiblemente llegó a ser un país más seguro debido a una mayor participación y liderazgo con la OTAN. Por otra parte, la guerra georgiana describe una historia muy diferente. Los ciberataques se coordinaron con la operación militar rusa y sirvieron de multiplicador de fuerza. Si bien los ataques en sí no tuvieron ramificaciones perdurables, la manifestación de fuerza posiblemente hizo que Georgia regresara a la esfera de influencia de Rusia. En ambos casos, los *hackers* rusos mostraron un admirable autocontrol en cuanto a la selección de sus blancos. En ninguno de los casos se seleccionaron infraestructuras críticas y el daño a largo plazo fue insignificante,[8] pero independientemente de esta búsqueda y selección de blancos de bajo nivel, los efectos psicológicos y económicos fueron considerables.

Departamento de Defensa, Cherie Cullen

El ex secretario de Defensa Robert M. Gates se dirige a la audiencia durante la ceremonia de activación del Comando Cibernético de EUA en el Fuerte Meade, estado de Maryland, 21 de mayo de 2010.

El segundo maestre Darrell Pierson observa mientras el marinero Seng Saeturn reconfigura el cableado de la red del Comando de Operaciones de Defensa Cibernética de la Armada.

Al conocer los escasos incidentes que hay en cuanto a guerra cibernética, los analistas se han visto obligados a especular sobre los usos y efectos de ataques de mayor envergadura y generales. ¿Cómo reaccionarán los estadounidenses ante los problemas ocasionados por un ciberataque estratégico como resultado de una intervención de Estados Unidos en el extranjero? Si bien no hay datos confiables en cuanto a cómo Estados Unidos reaccionaría ante graves dificultades ocasionadas por el conflicto, se puede sacar algunas conclusiones tentativas con respecto a la manera en que la opinión pública ha configurado el uso de la fuerza en las últimas dos décadas. Las conclusiones muestran que la aversión estadounidense en lo que se refiere a las bajas sufridas en la guerra se relaciona directamente a dos percepciones. La primera es que los estadounidenses necesitan estar convencidos de que lo que está en juego es importante. La segunda es que necesitan comprender que la probabilidad de lograr el éxito es alta. Si ninguna de estas dos condiciones se satisface, rápidamente se desvanece la tolerancia de bajas y el apoyo dado a las Fuerzas Armadas.[9] Esta tendencia fue ejemplificada en la campaña de Kosovo. En gran parte, la administración del presidente Clinton insistió en no desplegar fuerzas terrestres debido a las negativas repercusiones políticas que se sucitaron después del conflicto en Somalia. Si bien la campaña exclusivamente aérea fue eficaz, demuestra cuán lejos Estados Unidos está dispuesto a ir para evitar bajas.

Este bajo nivel de aceptación de bajas en el extranjero[10] se debiera traducir en una posición adversa aún más fuerte, si se toma en cuenta la amenaza que representa para los ciudadanos estadounidenses en Estados Unidos. De hecho, hay constancia de que, cuando se enfrenta una catástrofe interna, los gobiernos democráticos suelen retirar su apoyo a las misiones no vitales en el extranjero. Un reciente ejemplo se puede ver en el repliegue del Ejército español de Afganistán. Hay muchos que achacan los ataques terroristas contra las estaciones ferroviarias españolas como un evento catalizador por parte del Partido Socialista de Trabajadores para ganar el control del gobierno, que resultó en el repliegue de las fuerzas españolas de Afganistán. Las encuestas en España mostraron que la población en general jamás consideró que la guerra contra el terrorismo de Estados Unidos promovía la seguridad nacional de su país.[11] Además, los bombardeos en Madrid demostraron que, a pesar de tres años de guerra, ya era poca la probabilidad de lograr alguna forma de éxito concreto. El caso demuestra que las poblaciones civiles están más renuentes a correr riesgos si es muy probable que los costos involucrados les afecten directamente.[12]

La justificación de la Operación *Enduring Freedom* da aún más apoyo a este concepto de proteger la Patria contra cualquier riesgo. El argumento principal para la guerra con Irak fue el programa de armas de destrucción masiva (WMD, por sus siglas en inglés) del régimen de Saddam Hussein. La lógica fue que Estados Unidos y las fuerzas de la coalición debían invadir para desarmar a Irak e impedir la posibilidad de que Saddam atacara a Estados Unidos o a sus aliados. Esta posición oficial fue respaldada por las encuestas de opinión pública; a finales de mayo de 2003, más de 70% de los ciudadanos estadounidenses consideraron que la guerra estaba justificada.[13] Históricamente hablando, la población estadounidense ha apoyado las políticas intervencionistas que fueron analizadas como una manera de proteger la forma de vida estadounidense.

La previa discusión da una idea de las limitaciones en cuanto a la política exterior que

Estados Unidos enfrentará en el siglo XXI. Las capacidades cibernéticas podrían ser empleadas para ocasionar extensos daños económicos e incluso bajas civiles. El bombardeo de los trenes en Madrid que tan drásticamente alteraron el curso de la política exterior de España, podrían ser replicados, en gran parte, por medio de un ciberataque. La posibilidad de que un adversario cibernético con tecnología avanzada ocasione estragos en el territorio nacional de Estados Unidos es algo sin paralelo. Desde la guerra de 1812, ningún posible adversario ha podido atacar al territorio continental de Estados Unidos sin representar una amenaza existencial. Las capacidades cibernéticas son económicas, eficaces y podrían ser empleadas desde cualquier parte del mundo y en cualquier momento. La guerra cibernética probablemente representará un nuevo paradigma de fuerza que disminuye los casos de conflicto interestatales y reduce enormemente la intervención humanitaria armada debido al aumento de los costos transaccionales.

La seguridad hegemónica

La postura de Estados Unidos en cuanto a la defensa global desde el fin de la Segunda Guerra Mundial ha sido principalmente una de equilibrio en ultramar. En la más simplista de las perspectivas, Estados Unidos pasó el periodo de la Guerra Fría y las siguientes décadas intentando conservar los equilibrios de poder regionales e impidiendo que otra fuerza de coalición ganara una cantidad desproporcionada de poder. Dicho equilibrio ha ido del conflicto activo en Corea, Vietnam e Irak, a las actividades de apoyo en el Medio Oriente, África y el sudeste asiático. Desde la Segunda Guerra Mundial, Estados Unidos no ha peleado en un conflicto ni apoyado una política exterior intervencionista, en la que sus adversarios tuvieran la capacidad militar de ocasionar graves daños a Estados Unidos. De hecho, desde la guerra contra España, Estados Unidos no ha enfrentado fuerzas militares con un alcance global y bases militares a corta distancia del territorio continental de Estados Unidos con capacidad de ataque. La última vez que Estados Unidos fue invadido se dio en la guerra de 1812. Este impresionante aislamiento en lo que se refiere a conflictos se desvanece rápidamente según avanza la tecnología. Si bien Estados Unidos ha tenido la capacidad de actuar impunemente a nivel internacional, en gran parte debido a su posición geográfica, este no es el caso. Por primera vez en la historia, las capacidades cibernéticas permiten que los pequeños Estados con mínimos presupuestos de defensa, inflijan graves daños a un adversario mucho más fuerte desde grandes distancias.

Para dejarlo claro, las armas cibernéticas simplemente aumentan el costo del conflicto para los adversarios; es improbable que estas armas disuadan una política de seguridad nacional, si los intereses nacionales fundamentales están en juego. Salvo Estados Unidos y el Reino Unido, no hay otro país con una capacidad de proyección de poder global demostrada, que pueda aprovecharse de la situación creada por un ciberataque eficaz más allá de sus fronteras más cercanas. Por consiguiente, los ciberataques contra infraestructuras críticas principalmente se convierten en armas defensivas. Estas capacidades tienen el potencial de proporcionar una considerable seguridad al régimen a una fracción del costo de un programa de armas nucleares. Si bien el valor disuasivo puede ser menor que el de las armas nucleares montadas en misiles balísticos intercontinentales (*ICBM*, por sus siglas en inglés), un ciberataque tiene la posibilidad de infligir el suficiente daño para impedir una política exterior intervencionista. El costo de EUA para actuar como equilibrador en ultramar o como una fuerza de policía internacional, aumentará drásticamente. Es posible que esto erosione la tolerancia de los estadounidenses hacia las consecuencias generadas por la intervención en cualquier caso, salvo en circunstancias más extremas.

Las implicaciones

La importancia del equilibrio asimétrico convencional de fuerzas entre Estados Unidos y el resto del mundo es uno de los principales factores determinantes de este análisis y no se puede destacar lo suficiente. Según lo mencionado en previas secciones del presente artículo, las capacidades cibernéticas imitan, en gran medida, las repercusiones de las campañas de bombardeo estratégico de Estados Unidos. Las armas cibernéticas que se emplean contra infraestructuras críticas tendrán la capacidad

de compensar el resultado de los tradicionales ataques aéreos de una manera que Estados Unidos jamás ha experimentado. Es por eso que estas armas limitan, en gran medida, el uso de la fuerza estadounidense en el extranjero.

Hay tres posibles implicaciones de la llegada de calificadas armas cibernéticas. La primera es una restricción de coerción interestatal. Como una consecuencia de la primera, la segunda es la imposibilidad de implementar la iniciativa de seguridad humana, según lo argumentado por los partidiarios de la Responsabilidad de Proteger. Por último, las armas cibernéticas presentan la posibilidad de alterar, fundamentalmente, las estructuras de fuerzas convencionales.

El efecto más probable de las armas cibernéticas es el de disminuir radicalmente el uso de la violencia interestatal aprobada. Al igual que las grandes y capaces fuerzas convencionales, las armas cibernéticas presentan un fuerte elemento disuasivo al posible agresor. Las armas cibernéticas son una manera económica de desarrollar una capacidad de ataque global contra Estados conectados con las redes. Si bien Estados Unidos es el único Estado fuera del Medio Oriente que puede bombardear a Bagdad, muy pronto cualquier país conectado con las redes podría paralizar la capital de una nación. A raíz de esta capacidad, las políticas exteriores intervencionistas se harán sumamente costosas, no solo en términos de material y vidas de los militares, sino también en el territorio nacional. Los nuevos peligros que crea este quinto tipo de guerra, implica que solo los asuntos de seguridad nacional más importantes merecerán arriesgarse a los posibles ataques de represalia.

Esto lleva a una seria reconsideración de los conceptos de la seguridad global y de la iniciativa de seguridad humana, todo mientras ocasiona una disminución del sistema clásico westfaliano centrado en Estados. Si Irak o Yugoslavia hubieran desarrollado aún más sus capacidades cibernéticas, la probabilidad de ataques aéreos contra instituciones estatales hubiera sido radicalmente reducida. El costo de la intervención aumenta con la capacidad del Estado objetivo de lanzar un ataque cibernético exitosamente. ¿Cuántos Estados estarían dispuestos a evitar una crisis humanitaria, si el hacerlo significaría una pérdida de 5 a 7 por ciento de su propio Producto Interno Bruto (*PIB*),[14] aparte de los costos necesarios para llevar a cabo la acción militar? Además, a diferencia de los ataques preventivos con armas convencionales o nucleares que hipotéticamente pueden desarmar a un adversario, la naturaleza flexible e intangible del ciberespacio hace imposible tener cierta confianza con respecto a la eficacia del ataque preventivo. A diferencia de los otros cuatro tipos de guerra, es imposible ver una arma cibernética neutralizada en el ciberespacio. Ni las medidas ofensivas o defensivas pueden aliviar estos altos costos transaccionales con algún grado de certeza.

Por último, las armas cibernéticas pueden reducir, en gran medida, la necesidad de una gran fuerza aérea con alcance global. Este especialmente es el caso de los poderes emergentes o de los que enfrentan la necesidad de modernizar su inventario de aviones. Si bien la superioridad aérea aún es necesaria en una invasión y —por lo menos en el futuro cercano— para las operaciones de contra fuerza, su uso como arma estratégica va en rápido declive. Hay múltiples ventajas comparativas de las armas cibernéticas sobre los ataques aéreos. La primera y más convincente es el costo. Las armas cibernéticas cuestan una fracción de lo que cuestan los misiles y para entregarlas, no requieren plataformas de sistema complejos y costosos. Cualquier persona con una computadora portátil puede lanzar un ciberataque, mientras que los bombarderos *stealth* cuestan miles de millones de dólares. Aparte del costo, la naturaleza temporal de los ciberataques los hace mucho más atractivos si se toma en cuenta la reconstrucción pos guerra. Si un combatiente puede desactivar una planta eléctrica por cuatro días y, luego, con el toque de un interruptor nuevamente encender todas las luces, resulta inmensamente más económico y hace más fáciles los esfuerzos de reconstrucción, que bombardear una planta eléctrica y reconstruirla. Además, aunque puede haber efectos secundarios en la misma red, los ciberataques eliminan casi toda posibilidad de daños colaterales.

Estas implicaciones significan que es probable que cambie básicamente el futuro de la guerra y las limitaciones sobre la coerción internacional. La disuasión cibernética puede reducir los casos de violencia en el sistema internacional; sin embargo, también es probable que este tipo de disuasión

haga al mundo un lugar más seguro para regímenes corruptos y abusivos. Las armas cibernéticas —y su valor disuasivo— no compiten con las armas nucleares, sin embargo, tienen la capacidad de ser una mayor fuerza disuasiva que los sistemas convencionales. Puede que su valor disuasivo no sea significativo entre adversarios que luchan por intereses nacionales básicos, sin embargo, las capacidades cibernéticas ganarán mucha importancia cuando están en juego los intereses periféricos. Las mismas tienen la capacidad de subir los costos transaccionales de la guerra hasta el grado en que Estados Unidos, o cualquier sociedad avanzada, estaría mucho menos dispuesta a usar la fuerza internacionalmente basado en ideales o en percepción de equilibrio de poder regional marginal.

Los fracasos de la disuasión

Sin embargo, hay obvios problemas con respecto a la capacidad de disuasión en el ciberespacio. A diferencia de las armas nucleares o cualquier capacidad convencional, es casi imposible demostrar el poder cibernético. Además, es muy fácil desarrollar esta capacidad con una presencia física sumamente pequeña. La naturaleza técnica de las armas cibernéticas requiere que haya un problema preexistente en una parte específicia del software o la capacidad de asumir la identidad de un fiable usuario para llevar a cabo un ataque. En el ciberespacio, todo ataque termina en una defensa casi perfecta en solo días, o como máximo, en meses, lo que impide volver a usar esa específica acción. A diferencia de los sistemas de armas convencionales, las armas cibernéticas dependen de vulnerabilidades hechas por el hombre. No ejercen una destructiva fuerza física; más bien, operan como el agua que corre a través de una represa mal construida. El agua solo puede filtrarse si hay fisuras. Así mismo, las armas cibernéticas solo pueden penetrar las defensas de las redes, si hay fallas explotables en dichas defensas. Un ataque de negación de servicio distribuida (DDoS, por sus siglas en inglés), tal como los ataques contra Estonia y Georgia, pueden compararse con el agua que se derrama desde arriba de una represa. Si los

(Fuerza Aérea de EUA/Raymond McCoy)

El cadete de 1ª Clase Jordan Keefer, centro, coordina los esfuerzos de otros cadetes para defender su red durante el Ejercicio de la Agencia Nacional de Seguridad efectuado el 17 de abril de 2012. El equipo de la Academia de la Fuerza Aérea ganó el primer puesto en la competencia, superando a las otras academias militares estadounidenses así como a dos equipos egresados del Instituto de Tecnología de la Fuerza Aérea.

atacados detienen el flujo de actividad en Internet, el ataque DDoS será frustrado. Una vez que se realiza un ataque DDoS, es posible evitar que las computadoras empleadas para llevar a cabo el ataque vuelvan a atacar a Internet. Esto significa que todo ataque, incluso aquellos con propósitos ilustrativos, terminan siendo un sistema de armas irrepicable. Tal es así que la disuasión cibernética tiene una forma maquiavélica, casi completamente tipo *blind man´s bluff* [N. de T., una forma de juego de póquer no convencional en que una persona puede ver todos los naipes de los otros jugadores, pero no los suyos]. Estados Unidos no solo no sabrá si un posible adversario tiene las capacidades cibernéticas para infligir graves daños a la infraestructura crítica, sino que tampoco sabrá en qué punto dicho adversario se empleará las mismas. A medida que estas armas proliferan, a EUA se le hará cada vez más peligroso configurar activamente el ámbito internacional por medio de medidas coercitivas. No obstante, los políticos en Estados Unidos tendrán poca indicación de cuán grave será la amenaza que presentan estos países.

Sin embargo, hay algunos indicadores, aunque poco refinados, de cuán avanzado podría ser un ataque. Por ejemplo, frecuentemente se usan operaciones de inteligencia e intrusiones de bajo nivel para conocer la interacción de las redes. Trazar un mapa de una red eléctrica definida y otra infraestructura crítica es bastante útil, pero no es necesario para llevar a cabo un exitoso ciberataque. El gusano informático *Stuxnet* comprobó que siempre que un Estado tiene la capacidad de poner a prueba un arma cibernética en un sistema parecido a la composición de su blanco, puede ser muy exitoso. Por lo tanto, sería posible desarrollar un arma cibernética con solo una idea de las adquisiciones internacionales de los sistemas de control comerciales. En vista de que la mayoría de la tecnología necesaria para desarrollar complejas armas cibernéticas está disponible en el mercado libre y no está regulada, resulta imposible crear los tradicionales sistemas de control de tecnología y armas, ni verificar la adherencia a los mismos. Esto hace casi imposible rastrear el desarrollo de armas cibernéticas. De hecho, la única manera en que actualmente podemos estimar las capacidades cibernéticas de otro actor es midiendo la frecuencia y complejidad de los ataques que emanan de un Estado.[15]

(Armada de EUA, Segundo Maestre Jennifer R. Hudson)

El técnico de Sistemas de Información 2ª Clase David Coulter efectua una localización de problemas de una conexión satelital para los servicios de Internet a bordo del buque de asalto anfibio USS Bonhomme Richard (LHD 6).

La facilidad relativa con que un Estado, o incluso individuos, pueden desarrollar estas capacidades es suficiente para hacer pensar a los verdaderos expertos sobre el tema de seguridad.[16] Si esto se combina con la imposibilidad general de evaluar con precisión estas capacidades, es casi inevitable que Estados Unidos, o cualquier otro gran poder militar convencional, juzgue erradamente a su adversario, pagando por ese error un precio muy alto. Una vez que este particular Rubicón se cruce, el mundo no podrá dar vuelta a trás.

Conclusión

Las previamente expresadas doctrinas de estrategia militar pueden proporcionarnos un trayecto de desarrollo concreto para el uso de armas cibernéticas. Dada la similitud que existe entre el poder aéreo y el poder cibernético en cuanto a la adquisición y selección de blancos, es fácil deducir los aspectos paralelos y aceptar la doctrina del poder aéreo estratégico, como guía

principal en las primeras etapas del desarrollo de armas cibernéticas. Así mismo, los primeros debates sobre las armas nucleares y la disuasión son pertinentes, dependiendo de cómo las personas consideren la guerra cibernética. A pesar de estos vínculos, la singularidad de las armas cibernéticas hace que la puesta en práctica de teorías actuales sea una propuesta peligrosa que inhibe nuestra comprensión de cómo pueden y serán empleadas estas armas. Las armas cibernéticas tienen la capacidad singular de cambiar las relaciones internacionales de manera jamás antes vistas. La disuasión cibernética verdaderamente es la defensa económica. Un presupuesto de defensa medido en cientos de millones de dólares, eficazmente puede disuadir uno medido en cientos de miles de millones. Además, hoy en día, no hay leyes internacionales que rijan la adquisición o despliegue de estas armas. Por último, no se puede subestimar el peculiar impacto psicológico que producen las armas cibernéticas. La incapacidad que tiene una sociedad de resguardarse contra un inminente ciberataque incrementa los daños que inflige dicho ataque en la sociedad. La convergencia de estos factores crea una situación en donde las armas disuasivas son baratas y disponibles en el existente sistema internacional. Esto aumenta, en gran medida, la probabilidad de limitar la acción internacional de los países poderosos. Sin una defensa cibernética eficaz, será más difícil inducir el cambio a través del poder militar ofensivo. Las sociedades conectadas a las redes serán mucho más cautelosas al abogar por operaciones tales como intervención humanitaria, cambio de régimen, zona de exclusión aérea y demás operaciones de seguridad no esenciales. Si los intereses principales están en juego, es poco probable que los posibles daños físicos y psicológicos sean un factor disuasivo determinante para evitar el conflicto. Es posible que los altos costos relacionados con ese conflicto, hagan que los actores involucrados sean sumamente precavidos y exploren todas las posibles opciones antes de que la intervención se convierta en una opción viable.

Si las armas cibernéticas se desarrollan por esta línea, Estados Unidos y otros Estados avanzados conectados a las redes enfrentarán ventajas e inconvenientes. A diferencia de las armas nucleares y la guerra Fría, ningún país puede tener esperanza de desarrollar el suficiente poder ofensivo para disuadir el uso de las armas cibernéticas en ataques de represalia. La propia naturaleza de la disuasión cibernética, según lo antes descrito, está motivada por una abrumadora inferioridad convencional. El producir más capacidades ofensivas solo incrementará la probabilidad de que un pequeño Estado no espere para usar ataques desproporcionados en una crisis, o mejor dicho, antes de que sea disuadido. Además, si estalla un conflicto, desaparece cualquier esperanza de mutua disuasión cibernética. A diferencia del umbral que poseen las armas nucleares, las mismas vulnerabilidades que tentativamente permiten la disuasión cibernética, son blancos de suma prioridad de las campañas aéreas. Ya sea que un ataque aéreo incapacite o no, produce daños a la infraestructura crítica y no hay nada que evite que el Estado atacado desencadene un ataque cibernético a menera de represalia.

Esto le impone a Estados Unidos y a otros Estados avanzados estrictas consideraciones políticas; si bien no son mutuamente exclusivas, ninguna de estas opciones constituye una solución satisfactoria para este problema. En primer lugar, los Estados que dependen de la red, en un intento de crear defensas adecuadas, pueden recurrir a estrictos controles de la red, monitoreando todos los datos transferidos a un grado incluso mayor de lo que presenciamos en los países más reprimidos. En segundo lugar, los Estados podrían adoptar una estrategia solo de contra fuerza. Esto permitiría que los Estados aún tomen medidas militares, pero limiten sus acciones solo a ataques en contra del hardware específico de las fuerzas militares. Si bien, esto limitaría en gran parte la capacidad que tiene un Estado de efectivamente hacer la guerra, también ayudaría a crear un tabú contra los ataques en la infraestructura civil. Esto ayudaría a mitigar las vulnerabilidades del Estado interconectado a las armas cibernéticas e, incluso, le permitiría cierto nivel de libertad para intervenir en el extranjero. La última opción es simplemente aceptar que los costos transaccionales de la guerra han aumentado. Ninguna de estas opciones le resulta atractiva a un país que desea maximizar su flexibilidad para enfrentar los acontecimientos mundiales. Sin embargo, si se desarrollan las

armas cibernéticas —en la línea previamente descrita— forzará a que los estados activamente busquen, en distintos grados, todas las opciones anteriormente mencionadas.

Aunque es demasiado pronto para determinar si algunas de estas posibles tendencias se convertirán en realidad, estos asuntos ameritan un análisis más detallado. Con toda certeza, el valor de las armas cibernéticas cae en algún punto de un área gris entre un ataque nuclear estratégico y las fuerzas convencionales avanzadas optimizadas por la Fuerza Aérea de EUA. Si bien los teóricos de seguridad se apresuran a anunciar que los nuevos sistemas de armas son elementos transformadores, en el caso de las armas cibernéticas, la posibilidad verdaderamente existe. Las armas cibernéticas tienen una capacidad latente de marcar el comienzo de un nuevo orden internacional apoyado en la destrucción mutua asegurada, con base en bytes. Sin embargo, como ha sido el caso con todo anterior sistema, los espantosos efectos que producen las armas cibernéticas en el orden mundial solo se comprenderán cuando se empleen y el mundo pueda ver los efectos de primera mano. La siguiente década será crucial para el desarrollo de las armas cibernéticas y la forma de empleo por diversos Estados. Hasta que nosotros, como Nación y miembros de la comunidad internacional, verdaderamente comprendamos el uso completo de las armas cibernéticas en el sistema internacional, no podemos formular una política eficaz.***MR***

REFERENCIAS BIBLIOGRÁFICAS

1. Véase Conversino, Mark J., "The Changed Nature of Strategic Air Attack", para una discusión sobre la evolución del poder aéreo estratégico, publicado en la revista *Parameters* 27, nro. 4 (invierno de 1997-98): págs. 28-41.

2. En sus recientes comentarios ante el Congreso de EUA, el General Alexander ya ha declarado que algún tipo de disuasión basado en una vulnerabilidad mutua puede existir entre las naciones más poderosas.

3 Véase en informe de McAfee titulado "In the Crossfire: Critical Infrastructure in the Age of Cyberwar", disponible en Internet en: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf (accedido el 17 de abril de 2011), para más discusión sobre los blancos ya afectados; Lynn III, William J., "Defending a New Domain" *Foreign Affairs*, 89:5; *Lawrence Gershwin's Statement for the Record to the Joint Economic Committee on Cyber Threat Trends and US Network Security*, 21 de junio de 2001, disponible en Internet en: http://www.dni.gov/nic/testimony_cyberthreat.html (accedido el 17 de abril de 2011).

4. Clarke, Richard A., *Cyber War: The Next Threat to National Security and What to Do About It* (Nueva York: Harper Collins, 2010). Además, el Director Panetta, en sus comentarios ante el Comité de Inteligencia de la Cámara de Representantes de EUA, recientemente destacó que los ciberataques pueden paralizar al país.

5. Esta lista es solo ilustrativa. Cualquier aparato que está controlado, como mínimo, por una computadora, es vulnerable a las armas cibernéticas. Los sistemas con acceso a Internet son blancos más fáciles; sin embargo, el caso de Stuxnet demuestra que aún los sistemas *air-gapped* son vulnerables. (N. de T.: *air-gapped* es una red segura física, electrónica y electromagnética completamente aislada de las redes no seguras.

6. Una hipotética campaña cibernética podría desarrollarse de la siguiente manera: 1) choques aéreos de aviones de pasajeros civiles combinada con descarrilamientos de trenes AMTRAC de pasajeros o trenes subterráneo; 2) apagón de servicio celular; 3) rupturas de tuberías de gas, apagones de refinerías de petróleo e inundaciones utilizando las válvulas de seguridad de emergencia en represas; 4) el Estado que lanzó el ciberataque declara su responsabilidad; y 5) apagón de la red eléctrica nacional. La resultante pérdida de vidas, daños económicos y la percepción de victimización tiene la capacidad de destruir la voluntad de un Estado de continuar sus acciones ofensivas.

7. Ashmore, William C., "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review*, Tomo 11, 2009.

8. En el caso de Estonia, los blancos principales fueron los sitios web del Gobierno, grandes medios de comunicación y bancos. El modo de ataque principal fue la denegación de servicio distribuido (*DDoS*). En el caso de Georgia, los blancos principales también fueron los sitios web del Gobierno y los grandes medios de comunicación. La infraestructura crítica, tales como los sistemas SCADA que controlaban el oleoducto de Baku–Tbilisi–Ceyhan, no fue afectada. Parece que el propósito principal de los ciberataques era la guerra psicológica.

9. Larson, Eric V. y Savych, Bogdan, "American Public Support for U.S. Military Operations from Mogadishu to Baghdad" (Santa Monica, California: RAND Corporation, 2005), p. 219.

10. La conexión entre las bajas en el extranjero y las dificultades en EUA se ve acentuada por la transición a una fuerza totalmente compuesta de voluntarios. La falta de conscriptos traslada la carga del servicio militar de la sociedad en general a sectores minoritarios. El hecho de que los políticos aún reaccionan tan negativamente a las muertes de soldados estadounidenses a pesar de estar aislados, en gran parte, de los costos de la guerra, demuestra la gran aversión que hay en cuanto a las bajas.

11. En una encuesta sobre la post guerra en Irak realizada por Gallup International en Europa en 2003—63% de los encuestados opinaron que las acciones militares en Irak y Afganistán hicieron al mundo un lugar más peligroso.

12. El mejor ejemplo del paradigma de acción-reacción es el caso de España. A diferencia del 11-S, la población española consideró los bombardeos en Madrid una directa consecuencia del papel que jugaron en Afganistán, poniendo fin a las actividades de combate. El hecho de que la población vinculó su política exterior a la catástrofe en el territorio nacional demuestra la aversión de riesgos en general. En el caso del 11-S, los estadounidense se consideraron víctimas de un ataque no provocado. Esta diferencia en relación con la causa y efecto es fundamental para comprender cómo una democracia responderá a un ciberataque de gran escala.

13. Milbank, Dana y VandeHei, Jim, "No Political Fallout for Bus on Weapons," *The Washington Post,* 17 de mayo de 2003, http://www.washingtonpost.com/ac2/wp-dyn/A1155-2003May16 (accedido el 2 de abril de 2011).

14. Los cálculos basados en la presentación de Scott Borg en el 19º Simposio de Seguridad UESNIX titulado "How Cyber Attacks Will Be Used in International Conflicts (Cómo los ciberataques serán empleados en los conflictos internacionales)."

15. Este método no está perfeccionado y frecuentemente es poco confiable ya que que la mayoría de las pruebas forenses, en el mejor de los casos, puede rastrear el origen del ataque a una computadora específica. Esto no proporciona información alguna sobre el usuario de la computadora. El solo hecho de que un ataque se originó en un país no comprueba de manera fiable que un gobierno está involucrado. Por lo tanto, podemos ampliamente sobre o subestimar las capacidades verdaderas de un Estado, basado en esta métrica imperfecta.

16. Una breve búsqueda en Internet revela un sinnúmero de nuevas noticias sobre ataques por regímenes perversos que exhiben capacidades avanzadas, *hackers* adolescentes que usan métodos relativamente sencillos para ganar el control de la infraestructura crítica y artimañas de chantaje cibernético que afectan las redes eléctricas y refinerías de petróleo. Una reciente prueba de seguridad llevada a cabo por la seguridad de la tecnología de información de una planta de purificación de agua reveló vulnerabilidades letales y fácilmente explotables. Los ataques sobre la infraestructura crítica y sistemas del gobierno ocurren con inquietante frecuencia. Tal vez, la razón por la cual no hemos experimentado un ataque cibernético de gran escala, es porque la capacidad de los hackers es, en gran medida, limitada y el único motivo para seguir con el negocio es por razones intelectuales o económicas. Con base en estos acontecimientos, la extrapolación de lo que un Estado bien organizado y financiado podría hacer, no es significativa.