Spring March 1, 2014

La defensa cibernética fallida: Las consecuencias ambientales de actos hostiles.

Jan Kallberg, *University of Texas at Dallas*
Rosemary Burk, *Arkansas Tech University*

(FEMA, David Valdez)

La defensa cibernética fallida: Las consecuencias ambientales de actos hostiles

Jan Kallberg, Ph.D. y
Rosemary A. Burk, Ph.D.

UNA DEFENSA CIBERNÉTICA fallida puede tener efectos más generales que los tratados anteriormente en debates sobre las futuras consecuencias de un ataque cibernético. La necesidad de una defensa cibernética para proteger el ambiente no ha recibido la debida atención como un asunto de seguridad nacional. Los países adversarios secretamente buscan métodos para perjudicar y dañar a Estados Unidos mediante un conflicto cibernético futuro. El Presidente de Estados Unidos lo señaló en *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*:

Jan Kallberg es professor asistente en la Universidad Tecnológica Arkansas e investigador asociado en el Centro de Investigación y Educación en materia de Seguridad cibernética, Universidad de Texas en Dallas. Cuenta a su haber con un Doctorado de la Universidad de Texas, Dallas. Sus trabajos han sido publicados en varias revistas como Joint Force Quarterly, Strategic Studies Quarterly, Air and Space Power Journal, IEEE Access, e IEEE Security and Privacy.

Rosemary Burk es profesora asistente de biología en la Universidad Técnica de Arkansas. Cuenta a su haber con un Doctorado del Departamento de Biología en la Universidad del Norte de Texas. Sus trabajos de investigación han sido publicados por el International Journal of Water Resource Development y el Journal of Freshwater Ecology.

> "Ambos actores estatales y no estatales, poseen la capacidad y la intención de llevar a cabo espionaje cibernético y, potencialmente, ciberataques en EUA con efectos posiblemente graves tanto para nuestras operaciones militares como para nuestra patria".[1]

El ex secretario de defensa estadounidense, Leon Panetta, emitió una clara evaluación del riesgo de estos ataques en su discurso el 12 de octubre de 2012:

> "Estos ataques marcan un aumento significativo de las amenazas cibernéticas y han renovado las preocupaciones sobre los escenarios aún más destructivos que podrían desarrollarse. Por ejemplo, sabemos que los ciberactores extranjeros están probando las redes de infraestructura esenciales de Estados Unidos. Tienen como objetivo los sistemas de control de computadoras que operan plantas químicas, eléctricas y de purificación de agua, y los que guían las vías de transporte en todo el país.
>
> Sabemos de casos específicos donde los intrusos han ganado exitosamente acceso a estos sistemas de control. Además, sabemos que están intentando crear herramientas avanzadas para atacar estos sistemas y causar pánico y destrucción, e incluso, pérdida de vidas".[2]

Si bien, el liderazgo de la nación ha identificado el riesgo, expresó su preocupación y comenzó a asignar recursos para mejorar la defensa cibernética nacional, otros consideran marginal la probabilidad de una guerra cibernética. Uno de los principales argumentos contra la posibilidad de una futura guerra cibernética ha sido la premisa de que tal ataque no podría causar ningún daño a largo plazo.[3] Este argumento se basa en una marginación de los ciberataques como interrupciones intermitentes de computadoras de los clientes mediante un maligno *software* crudo y poco complejo que crea estragos temporales.[4] La percepción es que el daño se limita a las redes de computadora atacadas —no al ambiente externo que depende de las mismas. Sin embargo, las preocupaciones expresadas por Panetta, procedentes de la evaluación llevada a cabo por el Presidente, transmiten una percepción más general, más holística de los potenciales daños que van más allá de las redes informáticas.

En este artículo presentamos un argumento tangible de que esa guerra cibernética puede infligir daño continuo en una sociedad específica, más allá de la destrucción real de una red informática. Las consecuencias ambientales a largo plazo de una guerra cibernética nacional perdida y una defensa cibernética fallida, no son bien reconocidas. El estudio intenso de la última década en cuanto a la seguridad cibernética, con su énfasis en las redes y redes de seguridad, ha dejado el riesgo a ambientes que dependen de redes controladas cibernéticamente las cuales no han sido tratadas.[5]

El concepto de guerra cibernética

La guerra cibernética es un conflicto entre actores estatales que buscan un cambio de política en el otro partido. Por lo tanto, la guerra cibernética primero debe considerarse desde un punto de vista estratégico y segundo, desde los niveles inferiores de abstracción. Una parte central en todo conflicto es el temor a las consecuencias —las verdaderas repercusiones de la oposición a una voluntad que pretende dominar. Se temen las armas nucleares porque las mismas tienen efectos validados y devastadores gráficamente. Las armas cibernéticas necesitan mostrar que son catastróficas; de lo contrario, la amenaza o la disuasión del uso de las mismas se desvanece.

En estudios anteriores de la guerra cibernética, el foco estaba en las alteraciones de la capacidad técnica o militar y la resiliencia para operar en un ambiente degradado. El potencial de destruir sistemas contrarios a través de la letalidad digital ha sido recientemente presentada.[6] En estos escenarios, el daño a largo plazo es limitado. Las vulnerabilidades actuales en nuestros sistemas de control industrial resultan una oportunidad atractiva para un adversario que busca impactar la política estadounidense. Su objetivo puede tener impactos sociales significativos, temor, incertidumbre y presión pública sobre el liderazgo político, de producirse un daño ambiental.

El atacar los sistemas de control industrial para dañar el medio ambiente es un grave acto de guerra. Sin embargo, siempre y cuando la atribución sea desconocida y no haya ningún mecanismo punitivo vigente, las prohibiciones contra tales actos en el derecho internacional están sometidas a la discreción del atacante. En la actualidad, hay opciones limitadas, en caso de haber alguna, para reforzar la rendición de cuentas de los ataques cibernéticos a través del derecho internacional.

Los efectos ambientales de la guerra cibernética

Si un adversario puede producir grandes daños ambientales irreversibles a EUA a través de ataques cibernéticos en los sistemas de control industrial, o incluso, el control pre conflicto sobre numerosos sistemas, limitaría las opciones políticas de Estados Unidos. La amenaza y el riesgo de un ataque cibernético tendrían que ser considerados y le darían a una potencia menor el efecto multiplicador de fuerza en un conflicto directo con Estados Unidos.

La andanada de ataques cibernéticos en la infraestructura del país en la última década es merecedora de gran preocupación para el gobierno federal.[7] Estos ataques se han extendido hasta el punto de incluir los sistemas de control de supervisión y adquisición de datos (SCADA, por sus siglas en inglés), que son un subconjunto de los sistemas de control industrial. Los sistemas SCADA controlan los procesos en nuestra energía, transporte, administración de alcantarillado y agua potable, y otras industrias. Son la columna vertebral de la estructura técnica de nuestra sociedad. Los sistemas SCADA pueden permanecer viables durante décadas, dependiendo de los procesos y maquinaria que controlan estos sistemas. Sin embargo, a menudo, los sistemas SCADA carecen de capacidad o son difíciles de actualizar para enfrentar los desafíos contemporáneos de la seguridad cibernética. Muchos de estos sistemas jamás fueron concebidos ni diseñados para ser conectados a ninguna otra computadora, mucho menos vinculados a una red mundial de información como Internet. La gama de vulnerabilidades ha aumentado dramáticamente a medida que el *software* incorporado en maquinarias electromecánicas se ha convertido en una característica estándar. Estos controladores programables en la industria y compañías que proporcionan los servicios básicos tienen características limitadas de seguridad cibernética. La protección fortalecida y aumentada de los sistemas SCADA estadounidenses es probable que tome décadas; la mayoría de los sistemas SCADA no han sido actualizados desde que fueron instalados y necesitan otro *hardware* para hacerlos más seguros. La defensa de estos sistemas es una profunda defensa, donde tanto las corporaciones y los municipios como el Departamento de defensa son responsables junto con otras agencias federales. Los componentes más capaces de estas capas defensivas residen dentro de la esfera federal. La pregunta es: En caso de fallar la defensa cibernética, ¿qué podría suceder? Las ramificaciones ambientales no han recibido la debida atención en comparación con la amenaza potencial contra los sistemas computarizados.

Los diques y represas hidroeléctricas

Por ejemplo, un efecto en cascada de diques averiados en una gran cuenca tendría un impacto ambiental significativo. Los diques y represas hidroeléctricas son controlados mediante el uso de diferentes sistemas de redes de cable o inalámbricos y redes de control conectado a Internet. Una brecha en la defensa cibernética para la compañía de electricidad podría llegar hasta los controladores lógicos que instruyen a la maquinaria eléctrica abrir las compuertas. Muchos diques y represas hidroeléctricas están diseñados como una cadena de diques en una gran cuenca para crear un caudal de agua que se utiliza para generar energía. Un ataque cibernético en varios diques rio arriba podría liberar agua que aumentaría la presión sobre los diques rio abajo. Con la diminución rápida de la capacidad de almacenamiento, los diques rio abajo se verían comprometidos por el agua que se aproxima. Eventualmente, podría tener un efecto en cascada a través del sistema de río y resultar en una inundación catastrófica. La forma tradicional de seguridad cibernética para encuadrar el problema es considerar la pérdida

(Adam DuBrowa, FEMA)

La gran Tujunga Dam se encuentra bajo construcción para reforzar las paredes debido a los escombros aumentados que fluyen de las recientes tormentas de invierno. La Canada Flintridge, Calif., 2 de agosto de 2010.

de la función y la interrupción en la generación de electricidad —sin considerar el potencial efecto ambiental de un tsunami interno. Esto es especialmente problemático donde la población y las industrias son densas a lo largo de un río, como por ejemplo en los estados de Pensilvania, Virginia Occidental y otras áreas con ciudades desarrolladas en torno a molinos históricos. Si el ataque cibernético ocurre durante una lluvia severa cuando los diques ya están saturados, cualquier aumento rápido en el nivel del agua podría desencadenar un colapso en cascada.[8] Esto podría ocasionar una pérdida catastrófica de vidas y bienes y, la correspondiente pérdida de capacidad hidroeléctrica. Los efectos ambientales serían dramáticos y a largo plazo; los recursos de agua dulce se contaminarían, el ecosistema quedaría totalmente destruido, los agentes tóxicos se liberarían y el suelo quedaría erosionado en gran medida o completamente derrumbados. Las poblaciones de peces podrían ser diezmadas junto con la pesquería que depende de los mismos. Los efectos a corto y a largo plazo serían sustanciales y, los esfuerzos de restauración podrían ser demasiado costosos para el país. El daño del medio ambiente sería permanente.

La industria química de Estados Unidos

La considerable industria química de Estados Unidos ofrece otro ejemplo del potencial impacto ambiental de un ataque cibernético. Las fábricas e instalaciones de almacenamiento, albergan grandes cantidades de productos químicos industriales. La industria química estadounidense produjo US$ 759 billones de productos químicos en 2011.[9] Más de 96 por ciento de todos los productos manufacturados en EUA depende de material químico. Los Estados Unidos produce 15 por ciento de la producción química mundial. Todos los años, Estados Unidos transporta 847 millones de toneladas de productos químicos vía ferrocarriles, carreteras y buques de carga.[10] Las rutas de transporte están adyacentes o cerca de quebradas, ríos, acuíferos de agua subterránea, áreas urbanas y terrenos agrícolas. Estos fluidos químicos pueden, una vez liberados, crear una contaminación que requeriría una mitigación a largo plazo, restauración y, en algunos casos, hundimientos de tierra igual a un sitio superfondo de la Agencia de protección ambiental.[11]

Los productos químicos pueden infiltrarse en las aguas subterráneas y convertirlos en un peligro para la salud, contaminar el aire, contaminar el suelo y hacer los terrenos no aptos para la vivienda, agricultura ni desarrollo. Los daños podrían ser irreversibles, en caso de fallar la defensa cibernética.

La defensa del medio ambiente

La defensa de la infraestructura estadounidense contra los ataques cibernéticos no es solo proteger información, disponibilidad de la red o la red mundial de información. Además, es salvaguardar

la vida de los ciudadanos, la protección de bienes y la preservación de los ecosistemas y los servicios ecosistémicos de los que dependemos. Un ataque que produce daños al medio ambiente puede afectar la estabilidad de nuestra sociedad.[12]

La defensa cibernética nacional organizada por el Departamento de defensa y otras agencias del gobierno tiene una misión "verde" para garantizar que los ataques cibernéticos no ocasionen un daño ambiental irreversible en Estados Unidos. La defensa cibernética exitosa mitiga el riesgo de un daño significativo a fuentes de agua potable domésticas, ecosistemas acuáticos y terrestres adyacentes y protege la diversidad biológica. Esta misión debe continuar para proteger los recursos naturales esenciales para la vida.***MR***

Referencias Bibliográficas

1. Obama, Barack y Panetta, E., Leon, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Vol. 1 (Washington DC: Government Printing Office, 2012).

2. Panetta, E., Leon, "Defending the Nation from Cyber Attack" (speech given to Business Executives for National Security, New York, 11 de octubre 2012.)

3. Rid, Thomas, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): págs., 5-32.

4. Rid, Thomas y McBurney, Peter, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (2012): págs., 6-13.

5. Idaho National Laboratory, 2005, "US-CERT Control Systems Security Center," Cyber Incidents Involving Control Systems, INL/EXT-05-00671, disponible en http://www.inl.gov/technicalpublications/documents/3480144.pdf .

6. Kallberg, Jan y Lowther, Adam, "The Return of Dr. Strangelove," *The Diplomat*, 20 de agosto de 2012.

7. Lynn, E., William III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (2010): p. 97.

8. "Isaac leaves hundreds of homes underwater; dam shows stress," *Los Angeles Times,* 30 de agosto de 2012, http://articles.latimes.com/2012/aug/30/nation/la-na-isaac-storm-20120831.

9. American Chemistry Council, http://www.americanchemistry.com/Jobs/EconomicStatistics/Industry-Profile/Global-Business-of-Chemistry.

10. American Chemistry Council, http://www.americanchemistry.com/chemistry-industry-facts.

11. EPA. Superfund Sites, http://www.epa.gov/superfund/sites/npl/where.htm.

12. Kallberg, Jan y Thuraisingham, Bhavani, "State Actors's Offensive Cyber Operations-The Disruptive Power of Resourceful Systematic Cyber Attacks," *IEEE IT Professional* 15, no. 3 (2013): págs., 32-35.