Seguridad, Ciencia & Defensa, Año II, Nº 2, 2016, pp. 141-152

El Ejército y el desarrollo de capacidades para operar en el ciberespacio

THE ARMY AND THE DEVELOPMENT OF CAPABILITIES TO PERFORM IN CYBERSPACE

Recibido: 01 / 12 / 2016 ***Aprobado: 05 / 04 / 2017***

Alejandro Amigo Tossi

Oficial de Estado Mayor, Ejército de Chile. Master of Arts in Security Studies, Georgetown University. Magister en Conducción Militar, Academia de Guerra, Ejército de Chile. Licenciado en Ciencias Militares, Escuela Militar. Autor del blog "Ciberestrategia" https://ciberestrategia.wordpress.com/. Actualmente es parte del Grupo de Planificación Estratégica de la Dirección de Operaciones del Ejército de Chile. alejandroamigotossi@gmail.com

RESUMEN

La ocurrencia de diversos fenómenos en el ciberespacio y sus implicancias en la seguridad nacional han llevado a los actores estatales a identificar en ese ámbito una dimensión militar relevante, que demanda el desarrollo de capacidades para actuar en ese dominio del conflicto. Estas acciones requieren un enfoque estratégico que defina las funciones de todos los instrumentos del Poder Nacional. Una estrategia de seguridad en el ciberespacio que defina los modos y medios en este escenario, debe incluir el rol del Ejército para los fines diseñados por el Estado. Estas tareas deben considerar los desafíos asociados al ciberespacio como escenario de empleo de las Fuerzas Armadas y serán el marco para el desarrollo de las capacidades necesarias para dar respuesta a los distintos retos que impone el dinámico ciberespacio.

Palabras claves:

Ciberespacio, seguridad nacional, estrategia, ejército, desarrollo de capacidades.

ABSTRACT

The occurrence of various phenomena in cyberspace and its implications in National Security have led state workers to identify a significant military dimension in this field, which demands the generation of capabilities to act in of conflict domain. These actions require a strategic approach, which defines the roles of all instruments of National Power. A security strategy in cyberspace that defines the ways and means in this scenario should include the Army roles to achieve the ends designed by the state. These tasks should consider the challenges associated to cyberspace as another scenario for Armed Forces and will be the framework for the generation of the necessary means to confront different challenges imposed by dynamic cyberspace.

Keywords:

Cyberspace, national security, strategy, army, force generation.

Introducción

Según datos de fuentes públicas analizados por el Instituto de Investigación para el Desarme de Naciones Unidas (UNIDIR, por sus siglas en inglés), más de la mitad de los Estados poseen iniciativas para asegurar sus redes e infraestructura crítica y responder a las amenazas informáticas. De estos últimos, 47 Estados le dan roles a las Fuerzas Armadas y cuentan con planificación y organizaciones militares específicas para actividades en el ciberespacio. Además, al menos 27 de ellos han establecido entidades que tienen la responsabilidad de desarrollar operaciones en el ciberespacio y más de la mitad ejecuta capacidades ofensivas.

Estos datos demuestran que los Estados están asumiendo que las acciones en el ciberespacio tienen una dimensión militar relevante y que la tendencia es desarrollar capacidades para actuar en ese dominio del conflicto. De lo anterior, se deduce la importancia de desarrollar un enfoque estratégico que establezca las funciones y responsabilidades de todos los poderes del Estado en este ámbito.

La secuencia de planificación en el ámbito de la seguridad nacional indica que en la estrategia o política diseñada para ese efecto, se dispone el modo de empleo de los medios que disponen los Estados, para alcanzar el objetivo de promover los intereses nacionales. En esos documentos[1] además se señalan las principales amenazas que confrontarán para alcanzar sus fines, entre los cuales ciertamente serán incluidos diversos actores en el ciberespacio. La realidad actual en ese ámbito, en cuanto al nivel de frecuencia y peligrosidad de la acción de las amenazas, ha llevado a diversos Estados a establecer estrategias específicas para alinear los instrumentos del poder nacional en pos de los objetivos en el ámbito del ciberespacio. En ese marco, los Ministerios o Departamentos de Defensa deberán disponer tareas al Ejército, en concordancia con la realidad nacional y la respectiva cultura estratégica. Estas misiones o roles serán la referencia que guiará a la institución para el desarrollo de las capacidades necesarias para dar respuesta a los distintos desafíos que impone el dinámico ciberespacio.

1 Se emplea el término en plural, en atención a que los Estados disponen de políticas y/o estrategias para cumplir con el objetivo en comento.

El objetivo del artículo es describir los desafíos inherentes al rol del Ejército en el marco de una estrategia de ciberseguridad nacional y las consideraciones para el desarrollo de las necesarias capacidades que darán cumplimiento a esas tareas. Para lo anterior, en primer término se describirá brevemente el ciberespacio como un nuevo escenario de empleo; luego, se analizarán los retos que impone al Ejército emplear sus medios en el ámbito descrito; posteriormente, se establecerán los principales lineamientos que debieran contemplar las capacidades requeridas para lograr los fines proyectados en el ciberespacio, que deberán considerar entre otros aspectos, las técnicas para ejecutar ciberoperaciones, la organización, el personal, la doctrina de empleo y la infraestructura necesaria.

Escenario

Ciberespacio

Según la Unión Internacional de Telecomunicaciones, el ciberespacio es "el terreno físico y no físico compuestos por alguno o todos los siguientes elementos: computadores, sistemas informáticos, redes y software, datos de contenido y tráfico y por último, los usuarios". Esta definición implica que el ciberespacio está conformado por tres componentes interdependientes:

- El componente humano: usuarios de las computadoras y los sistemas informáticos.
- El componente lógico: correspondiente a internet, con sus correspondientes softwares y bits. Estos últimos se mueven a la velocidad de la luz y representan la información, las instrucciones, softwares, malwares y otros tipos de virus. En este componente es importante destacar la "Deep web" que corresponde a la información en Internet que no es accesible a través de los buscadores normales. Esta sección de internet corresponde a la totalidad de información oculta y de restringido acceso para la gran mayoría de los usuarios de internet. Los principales sitios y actividades corresponden a redes privadas de organizaciones que requieren claves para su acceso, blogs de movimientos y organizaciones que buscan la reserva de sus comunicaciones, y sitios de diversos tipos y orígenes donde además, ocurren todo tipo de actividades delictivas.
- El componente físico: hardware, equipamiento móvil, fijo e infraestructuras terrestres, marítimas, aéreas y espaciales.

La Amenaza en el Ciberespacio

La ciberamenaza considera un amplio espectro de actores representados principalmente por actores estatales (a la fecha no hay casos de reconocimientos explícitos), "hacker patriotas", "hacktivistas", terroristas, cibercriminales e "insiders". Éstos emplean diversos tipos de métodos y sus objetivos se extienden desde actividades de ataque y exploración de redes informáticas, ciberespionaje, cibercrimen, apoyos a movimientos civiles y difusión de información clasificada. En las técnicas empleadas por éstos, encontramos la acción de virus en sistemas informáticos, denegación del servicio en sitios web, robo de información sensible, eliminación de la información en computadores y bases de datos y la inutilización de sistemas de control de infraestructura crítica.

Estos hechos precisan un enfoque integral para comprender la complejidad del fenómeno y los retos que plantean a los actores estatales, considerando que el avance tecnológico de los Estados traerá como consecuencia que éstos deberán lidiar con mayor frecuencia con una ciberamenaza adaptativa y de creciente complejidad. Además, la proliferación global de códigos maliciosos o malwares ha aumentado el riesgo contra las redes y datos; un Estado o actor no estatal puede adquirir malwares y otros códigos en la Deep Web o externalizar la detección de vulnerabilidades en las redes objetivos. Por tanto, para ejecutar una operación cibernética perjudicial en contra de un sistema informático sólo se requieren conocimientos y no sería

necesario un alto gasto de recursos para desarrollar capacidades ofensivas.

Desafíos para el Ejército

CIBERESPACIO COMO DOMINIO DEL CONFLICTO

Existen implicancias para la planificación de empleo de los medios del Ejército, si consideramos al ciberespacio como una nueva dimensión del conflicto. Denominado como el quinto dominio, sumándose al ámbito terrestre, marítimo, aéreo y espacial; el ciberespacio, es transversal a los otros y las redes y sistemas de información que lo componen, son claves en la articulación de las acciones que ocurren en los otros y por tanto, su control y seguridad afectará la conducción de las operaciones militares.

El ciberespacio es una dimensión del conflicto modificable, a diferencia de los otros ámbitos. Al corresponder a una creación humana, se puede configurar un ciberespacio ajustado a la respectiva realidad nacional, que aumente o disminuya los niveles de seguridad, su tamaño y las complejidades para su acceso. Al respecto, es posible afirmar que existen dos grandes segmentos de países en cuanto a su capacidad de emplear para sus fines el ciberespacio. Primero, aquellos tecnológicamente avanzados y que sus sistemas dependen masiva y primordialmente de la conexión a redes, y aquellos que no han alcanzado esa condición por no poseer los recursos y las tecnologías. De esta forma, los Estados más avanzados transformarían a su ciberespacio en un objetivo de alto valor, mientras que en los otros casos, no sería de mayor relevancia atacar el disminuido uso que estarían haciendo del ciberespacio.

Otra característica del ciberespacio es su compartimentaje virtual. Es decir, podría plantearse la existencia de un ciberespacio propio, de la amenaza y otro público de libre acceso. En los dos primeros casos, corresponde a las redes de los actores estatales conectadas o no a Internet, donde operan sus sistemas de acceso restringido; la tercera parte corresponde a todos los sitios de acceso universal. Es decir, el ciberespacio no es unitario, sino que esta subdividido en varias áreas que incluso pueden ser ajustadas por los usuarios. Estos hechos permiten descartar la idea de la supremacía en este nuevo dominio, y por tanto, la utopía de pensar que si se controla el ciberespacio se domina el resto de los dominios del conflicto.

Ciberguerra[2]

La política y/o estrategia de defensa nacional debe considerar a las acciones en el ciberespacio como otra categoría de las tareas que materializan el empleo de los instrumentos del poder nacional para la consecución de los objetivos políticos del Estado. Es decir, la denominada "ciberguerra" no es un ámbito de acción independiente, sino que acontecerá en el marco de un conflicto (no necesariamente en el marco de una crisis y/o de tipo bélico), que le brinda el contexto para su desarrollo. Lo anterior, ha sido evidente cuando Estados han empleado ciberoperaciones como una herramienta de coerción y un elemento complementario al uso de la fuerza en escenarios de conflicto. Este ha sido el caso de la estrategia Rusa en el conflicto de Ucrania, donde se ha utilizado una combinación de acciones que implican el uso coactivo y coercitivo de fuerzas mediante tácticas no convencionales, empleo de fuerzas irregulares,

2 Se empleará este fenómeno en forma genérica para identificar las acciones que las fuerzas armadas, en este caso el Ejército, desarrollará en el ciberespacio.

acciones encubiertas, manipulación política y ciberoperaciones.

Por otra parte, es importante definir que la prioridad de las ciberoperaciones debe ser el aporte al logro del objetivo determinado para el empleo de la fuerza, siendo la protección del ciberespacio, es decir de la información, una acción que coopera a lo anterior y no es el fin de las operaciones.

Ciberespacio y el uso de la fuerza

En los otros dominios del conflicto, una agresión que involucre el uso de la fuerza será respondida con una acción similar por parte del actor víctima. Sin embargo, en el ciberespacio esta lógica posee una mayor complejidad. Por ejemplo, en caso de definir con certeza al agresor, ¿cual sería el objetivo por alcanzar con una respuesta militar? ¿destrucción de computadores y/o redes del actor responsable?, ¿eliminación de información?, etc.

Considerando que un ciberataque podría crear efectos físicos equivalentes a un ataque armado, este tipo de capacidades no deben ser analizadas solamente desde la perspectiva del efecto físico. Su condición particular, conllevará dificultades al momento de evaluar si un incidente cibernético puede ser considerado como uso de la fuerza. Una posibilidad es que el efecto de la acción sea equivalente a un ataque con armas convencionales que producen destrucción física o bajas, ya que la ocurrencia de lesiones o muertes de personas y la destrucción o daño de la propiedad, evidentemente serían considerados como un ataque armado.

Disuasión

Las operaciones cibernéticas permiten a los Estados ejecutar acciones ofensivas con un menor riesgo político, un conveniente grado de ocultamiento y en un contexto ambiguo de la legalidad internacional, respecto a si esas acciones se estiman como un "ataque armado" que legitimaría una respuesta. Por tanto, para alcanzar un grado de disuasión creíble y efectiva en el ciberespacio se requerirá una serie de herramientas para negar el éxito al adversario y ser capaz de afectar sus operaciones. Entre otras, la articulación de elementos de respuesta eficaces para disuadir a un adversario de iniciar un ataque; capacidades defensivas para impedir el éxito de un ataque potencial y el fortalecimiento de la resiliencia de los sistemas anteincidentes. Además, se demandará una dinámica inteligencia, aptitudes forenses, sistema de alarmas y métodos para reducir el anonimato en el ciberespacio y aumentar la probabilidad de atribución.

Al respecto, la atribución es fundamental para una disuasión eficaz, a través de la identificación de los ataques y de las tácticas, técnicas y procedimientos empleadas. La acción de determinar al responsable de un ciberataque debe relacionarse con el objetivo del ataque y en el contexto de un conflicto o crisis en curso, o además, con acciones similares anteriores. El caso del ataque a la empresa Sony por parte de un grupo de hacktivistas que explicitaron defender los intereses Norcoreanos, es un ejemplo donde la supuesta atribución se facilita por el contexto y el objetivo de los ataques perpetrados.

A la fecha, la totalidad de los casos que se han hecho públicos, los supuestos actores responsables han negado la situación y por tanto, ha sido complejo para las naciones víctimas ejecutar acciones de respuesta o promover algún

tipo de sanción internacional, debido a la ausencia de normas reconocidas globalmente en el dominio del ciberespacio.

Superioridad de la ofensiva

La evidencia sobre las acciones de elementos hostiles en el ciberespacio, genera la percepción que sus capacidades son siempre capaces de superar las previsiones de seguridad y protección de sus objetivos. Es decir, a pesar de las medidas que se adoptan en materias de ciberseguridad en los sistemas informáticos, éstos van a permanecer siempre, en menor o mayor grado, a merced de las incursiones o ataques externos con distintas motivaciones y objetivos.

Esta realidad manifiesta una superioridad de las acciones ofensivas, creando una situación donde las organizaciones no debieran estimar "si" serán víctimas de ataques, sino, "cuando" y "cómo" sus sistemas serán vulnerados. Más aún, si la principal agencia de inteligencia de EEUU ha sido víctima de intrusiones cibernéticas, es posible afirmar que ninguna organización puede alcanzar un grado de seguridad que las haga impenetrables o inmunes. La permanente creación de softwares con elevados estándares de seguridad y la consecuente difusión periódica de parches, sólo representan una disminución momentánea de los niveles de riesgo cibernético.

Capacidades por desarrollar

Las capacidades que el Ejército debe desarrollar para cumplir sus tareas en el ciberespacio,se conforman sobre la base de los siguientes elementos: personal, la doctrina para su empleo, una estructura organizacional que las ejecute, infraestructura física que la sustente y como elemento primordial, los software y/o técnicas que materializan las ciberoperaciones.

Personal

La preparación del personal para el empleo en el ciberespacio debe corresponder a uno de los primeros pasos del proceso. La educación de los futuros responsables de planificar y emplear las distintas herramientas disponibles en este ámbito debe abarcar todos los niveles. Se requerirá personal capacitado para planificar operaciones en el ciberespacio en el marco del empleo de la fuerza ante la crisis y/o conflicto, como también para la seguridad de las redes en el funcionamiento diario institucional. Se demandarán asesores de alto nivel y los comandantes de las entidades especializadas responsables de lidiar con la permanente amenaza que plantea el ciberespacio. Además, se debe capacitar a los que ejecutarán las operaciones que permitirán proteger el ciberespacio propio y las acciones que se dispongan en las redes adversarias. Esta formación debería desarrollarse en un ambiente conjunto e interagencial con el objeto de preparar al personal con una visión integral sobre el rol de los distintos actores en la estrategia de ciberseguridad nacional. En estas instancias será vital la participación de la comunidad académica y científica con el objeto de considerar las últimas tendencias y avances tecnológicos sobre el tema.

Doctrina

La elaboración del marco doctrinario que orientel a ejecución de operaciones en el ciberespacio, debe fundamentarse en los marcos legales nacionales con el objeto de que los contenidos de esos textos cumplan con esas normas. Este proceso debiera iniciarse en el nivel conjunto y desde ese escalón, alinear los cuerpos doctrinarios de las respectivas Fuerzas Armadas y por tanto, del Ejército. La doctrina debe establecer el marco de empleo de las operaciones en el ciberespacio, es decir, definir si se enmarcarán en conceptos tales como, las operaciones de información, guerra de información y/u operaciones de carácter híbridas [3].

Además, esta doctrina debe precisar entre otros, los siguientes aspectos: la relación entre la función inteligencia y las operaciones en el ciberespacio, la correlación entre el ciberespacio y el espectro-electromagnético, las actividades que definen las operaciones en redes y sistemas computacionales y la contribución de estas acciones en el campo de batalla.

Estructura organizacional

La ejecución de las tareas asignadas al Ejército en el ciberespacio exigirá la conformación de estructuras organizacionales que permita la operacionalización de las capacidades. En primer lugar, será necesario definir las responsabilidades del escalón conjunto y de las respectivas ramas de la defensa nacional, en particular las del Ejército. En segundo lugar, será necesario concebir la integración de los roles institucionales con las actividades del ministerio o departamento de defensa y los otros sectores del Estado con responsabilidades en el ciberespacio, para evitar superposición de misiones, coordinar sistemas de seguridad y reportes, compartir experiencias y elevar estándares de seguridad de manera colectiva.

Por último, la evidencia internacional sugiere la creación de organismos para dirigir, controlar y coordinar las actividades asignadas al Ejército. Al respecto, en el plano operativo y/o técnico, un aspecto generalizado es la formación de Equipos de Respuesta ante Emergencias Computacionales o CERTs para la protección de la infraestructura crítica institucional.

Capacidades técnicas

Las ciberoperaciones son la parte principal de las capacidades a ser desarrolladas por el Ejército. Estas operaciones tienen por objetivo mantener la seguridad de los sistemas propios y el ataque y explotación de las redes y sistemas de potenciales adversarios. En casos de crisis y/o conflicto estas acciones se integrarán en la estrategia diseñada para obtener la superioridad militar en una determinada área de operaciones. La literatura sobre el tema, por lo general, las desagregas en defensivas, ofensivas y de exploración.

Defensivas

El objetivo principal de estas ciberoperaciones es asegurar la confidencialidad, disponibilidad e integridad de la información que permiten al Ejército cumplir con sus tareas fundamentales diarias y/o en caso de crisis o conflicto bélico, derrotar al adversario en el campo de batalla. Estas

3 Conceptos correspondientes a distintas formulaciones doctrinarias que incluyen a las operaciones en el ciberespacio.

acciones deben confrontar una amplia gama de intrusiones, desde entradas para reunir información de inteligencia hasta ataques. Las ciberoperaciones defensivas corresponden a una serie de medidas para disminuir los riesgos informáticos y mitigar la superioridad de la ofensiva. Un aspecto vital son las políticas de ciberseguridad que involucran a todos los niveles de la organización y consideren las características de las amenazas. Estos procedimientos permitirán coordinar las acciones que incrementarán la prevención, protección y recuperación ante ataques. Además, están las iniciativas de carácter eminentemente técnico aplicadas al software y hardware que componen los propios sistemas. Asimismo, es importante poseer capacidades de investigación forense para identificar responsables de intrusiones y las técnicas utilizadas.

Otro aspecto a contemplar es el desarrollo de capacidades para una defensa activa, es decir, afectar al actor malicioso en el lugar físico desde donde está operando; sin embargo, la existencia de malwares "fire and forget" ("Stuxnet"), el empleo de robots o botnets y la deep web degradan la efectividad de esas acciones ante adversarios sofisticados.

La ejecución de estas medidas defensivas, con una mayor o menor preponderancia de algunas de ellas, serán las acciones que permitirán alcanzar un grado de seguridad relativa ante la constante amenaza cibernética, que encuentra ambientes menos o más proclives.

Ofensivas

Si así considera la respectiva estrategia de ciberseguridad nacional, el Ejército debería adquirir o desarrollar capacidades para ejecutar operaciones cibernéticas de tipo ofensivas. Las tecnologías empleadas en el ciberespacio tienen aplicaciones militares que pueden ser explotadas en situaciones de conflicto. Para periodos distintos a la crisis y/o conflicto, la Institución podría asumir roles en la exploración de sistemas informáticos adversarios. En casos de empleo coactivo o coercitivo de la fuerza, estas operaciones tendrán como finalidad interrumpir los sistemas de mando y control de potenciales adversarios para reducir su capacidad de controlar operaciones en los otros dominios de la guerra, la degradación de sistemas de armas que se basen en sistemas informáticos, destrucción de bases de datos, "denegación de servicio" contra sitios web para interrumpir su funcionamiento e inutilización de infraestructura crítica de uso militar. Otras tareas a desarrollar son la búsqueda del control de la información pública en la respectiva zona de conflicto y acciones de propaganda hacia determinados grupos objetivos a través de redes sociales y medios de información pública.

Exploración

Estas capacidades tienen como propósito obtener información sobre las actividades, recursos de información o las capacidades de los sistemas objetivos. Estas operaciones permiten obtener una ventaja decisiva de información en relación a las potenciales amenazas al Estado y en este caso, al Ejército. Si bien estas acciones se deben desarrollar desde la paz, de manera específica para el rol del Ejército esas operaciones preparan el campo de batalla en el ambiente informático, es decir, exploran las redes y sistemas de mando y control que configuran ese espacio, detectan sus fallas y en caso de ser requerido, proceder a desarrollar operaciones de tipo ofensivas. Otras acciones estarán relacionadas con la obtención de información contenida en esas redes, con el fin de comprender ciertas capacidades de la amenaza, anticipar sus acciones y defenderse de potenciales ataques a las propias redes.

Conclusiones

La constante computarización y automatización de los procesos como efecto de la creciente disponibilidad de tecnologías que permiten mejorar el funcionamiento y gestión de las organizaciones, genera una progresiva exposición a las acciones maliciosas que buscan afectar los sistemas. Este fenómeno afectará a todos los ámbitos del Estado y por tanto, a todos los estamentos que lo componen.

El Ejército, como integrante de las Fuerzas Armadas, es parte del Poder Militar de los Estados, y por tanto, deberá cumplir las tareas contempladas en la estrategia de ciberseguridad nacional que permitirán alcanzar la condición deseguridad proyectada en el ciberespacio propio. El rol del Ejército dependerá de la cultura estratégica de los respectivos Estados, del ámbito de acción asignado a cada sector u organismo público, del grado de desarrollo de la institución en el ciberespacio y de las lecciones aprendidas relacionadas con incidentes informáticos.

Las tareas asignadas a la institución en la respectiva estrategia de ciberseguridad, corresponden a la referencia principal para las capacidades que debe desarrollar el Ejército, las que deberán ser financiadas con los recursos suficientes para su operación y mantención. Estas capacidades deben ser diseñadas para ser ejecutadas en períodos de paz, crisis y durante las distintas etapas de un conflicto. Es decir, el personal y la estructura organizacional que ejecutan las ciberoperaciones, deben apoyar el empleo operacional del Ejército en los potenciales escenarios de empleo, como asimismo, proteger el funcionamiento diario de los sistemas informáticos de la institución que soportan sus permanentes procesos de preparación y apoyo.

Bibliografía

Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. OTAN.

Cornish, P., Livingstone, D., Clemente, D., y Yorke, C. (November 2010). *On Cyber Warfare*. Chatham House Report. pp. 8-9.

Even, S. and Siman-Tov, D. (May 2012). Cyber *Warfare: Concepts and Strategic Trends*. Memorandum No. 117 Institute for National Security Studies.

Eronen, P. (June, 2016). *Russian Hybrid Warfare: How to confront a new challenge to the West*. Foundation for Defense of Democracies. Washington, DC.

Giles, K.; Hartmann, K. (September 2015). Cyber Defense: *An International View. The Letort Papers*. Strategic Studies Institute and U.S. Army War College Press.

ITU Toolkit for Cybercrime Legislation, p. 12. www.itu.int/cybersecurity.

Libicki, M. (Fall 2012). Cyberspace is not a warfighting domain. *Journal of Law and Policy for the Information Society,* 8 (2).

Melzer, N. (2011). Cyber warfare and international law. *UNIDIR Resources.*

United Nations. Institute for Disarmament Research. (2013). *The Cyber Index: International security trends and realities.* Geneva, Switzerland.

US Department of Defense. (November 2010). JP 1-02, Department of Defense. *Dictionary of Military and Associated Terms.*

United States Government. (April 2015). The Department of Defense Cyber Strategy.

http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0

https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html.