Guía Comité de Desarme y Seguridad Internacional
(DISEC)
Presidente: Valentina Díaz
Copresidente: Juliana De Las Salas

Introducción a DISEC

El Comité de Desarme y Seguridad Internacional se creó por primera vez en la Carta de las Naciones Unidas, en el Capítulo IV, con la intención de defender, debatir y resolver cuestiones de desarme y seguridad internacionales. DISEC también se conoce como el Primer Comité de la Asamblea General de las Naciones Unidas. Según el Artículo 9 de la Carta de las Naciones Unidas, todos los 193 miembros de la ONU pueden ser elegidos como representantes en DISEC y tienen voto igualitario. Es importante tener en cuenta que DISEC, si bien se ocupa de cuestiones de seguridad importantes, **no puede exigir específicamente medidas estatales individuales, sanciones o intervención armada**. DISEC, sin embargo, puede recomendar todas estas acciones al Consejo de Seguridad.

Tema A: Medidas Globales de Lucha contra el Terrorismo

La amenaza de la violencia causada por ideales extremistas, ya sean justificados por asuntos ideológicos, políticos, religiosos o económicos, siempre ha sido un tema de extrema importancia dentro las Naciones Unidas e incluso precede esta organización. Las acciones terroristas han variado a través de la historia, pero todas tienen un denominador común: su crueldad extrema. La amenaza del terrorismo actual peligra la seguridad de la comunidad internacional y la integridad de sus habitantes de maneras nunca antes vistas.

El terrorismo existía antes de que la palabra misma fuera inventada. Hay muchas definiciones de terrorismo pero no existe una que este universalmente aprobada. El libro "¿Qué es el terrorismo?" de Johathan Matusitz expone distintas definiciones de varios expertos e instituciones, entre ellas:

- **Walter Laqueur:** "El terrorismo es el uso o la amenaza del uso de la violencia, un método de combate o una estrategia para alcanzar ciertos objetivos ... Tiene como objetivo inducir un estado de miedo en la víctima, que es despiadado y lo hace no se ajusta a las normas humanitarias ... La publicidad es un factor esencial en la estrategia terrorista"
- **Bruce Hoffman:** "El terrorismo es ineluctablemente político en objetivos y motivos, violento o, igualmente importante, amenaza la violencia, diseñado para tener repercusiones psicológicas de largo alcance más allá de la víctima o el objetivo inmediato, llevado a cabo por una organización con una cadena de mando identificable o estructura de célula conspirativa (cuyos miembros no llevan insignias uniformes o de identificación), y perpetrada por un grupo subnacional o una entidad no estatal."

Como cada nación lo define de manera diferente, esto explica por qué ciertos países definen algunos grupos como grupos terroristas mientras que otros no. Según Yasser Arafat, ex presidente de la Organización de Liberación de Palestina, "cualquiera que defienda una causa justa no puede ser llamado terrorista".

Ataques Recientes

1990's

- **1997:** Ataques suicidas en Israel mataron a una docena de personas e hirieron a más de 150; Un tiroteo en India mato a 23 e hirió a 31.
- **1998:** Miembros de Al-Qaeda bombardearon dos embajadas americanas, dejando 200 muertos y 4000 heridos.
- **1999:** Bombardeos a apartamentos en Rusia suroriental dejaron 300 muertos y más de 1000 heridos

2000's

- **2001:** El 11 de Septiembre, las Torres Gemelas fueron derribadas por un avión secuestrado, dejando a más de 2,700 heridos. Otros aviones habían sido mandados al Pentágono, El Capitolio y La Casa Blanca.
- **2004:** Bombas puestas en trenes en Madrid mataron a mas 200 e hirieron a más de 2000.
- **2005:** Un carro bomba en Iraq dejo a cientos de heridos y mato a 127. En Julio de ese mismo año, cuatro bombarderos suicidas atacaron un bus en Londres, dejando a más de 700 heridos.
- **2006:** Servicios de seguridad británicos, frustraron un complot de Al Qaeda. Más de una docena de ciudadanos británicos de origen paquistaní fueron entrenados para mezclar explosivos en aviones en ruta desde Heathrow a media docena de aeropuertos en Canadá y Estados Unidos, volando simultáneamente sobre el océano Atlántico norte. Tenía como objetivo conmemorar el quinto aniversario del 11 de septiembre con asesinatos en masa aéreos, lo que llevaría al colapso del negocio de las aerolíneas globales y la economía global.

2010's

- **2012:** Damasco y Alepo en Siria se volvieron epicentros de la actividad terroristas, y las ciudades han sido destruidas hasta la fecha.
- **2013:** Las bombas en la Maratón de Boston dejaron 5 muertos y 200 heridos.
- **2015:** Un ataque de ISIS en las oficinas de la revista Charlie Hebdo y cuatro otros ataques en Paris mataron a 17 personas.
- **2016:** Un tiroteo en un bar LGBT+ en Orlando dejo a 50 muertos, siendo la tragedia más grande en la historia de E.E.U.U, y el peor ataque terrorista desde 9/11.
- **2017:** Una bomba suicida a la salida de un concierto de Ariana Grande en Manchester dejo a 23 muertos, incluido el atacante, quien tenía lazos con ISIS.

Acciones Internacionales

La Asamblea General aprobó la **Estrategia Global de la ONU Contra el Terrorismo**. Esto implicó un consenso entre todos los miembros, de un enfoque estratégico común, no sólo enviando un mensaje claro de que el terrorismo es inaceptable en todas sus manifestaciones sino también decidiendo dar pasos prácticos a nivel colectivo para prevenir y combatirlo.

Desde 1963, la comunidad internacional ha promulgado 19 instrumentos internacionales para prevenir actos terroristas. Entre ellos están:

INSTRUMENTOS RELACIONADOS CON LA AVIACIÓN CIVIL

I. *Convención de 1963 sobre infracciones y ciertos otros actos cometidos a bordo de aeronaves*
II. *Convenio de 1971 para la represión de actos ilícitos contra la seguridad de la aviación civil*
III. *Convenio 2010 sobre la supresión de actos ilícitos relacionados con la aviación civil internacional*

INSTRUMENTOS RELATIVOS A LA PROTECCIÓN DEL PERSONAL INTERNACIONAL

IV. *Convención de 1973 sobre la prevención y el castigo de delitos contra personas internacionalmente protegidas*

INSTRUMENTO RELATIVO A LA TOMA DE REHENES

V. *1979 Convención internacional contra la toma de rehenes*

INSTRUMENTOS RELATIVO A LA NAVEGACIÓN MARÍTIMA

VI. *Convenio de 1988 para la represión de actos ilícitos contra la seguridad de la navegación marítima*

INSTRUMENTO RELATIVO A LOS MATERIALES EXPLOSIVOS

VII. *Convenio de 1991 sobre el marcado de explosivos de plástico con fines de detección*

INSTRUMENTO RELATIVO A LOS BOMBARDEOS TERRORISTAS

VIII. *Convenio internacional de 1997 para la represión de los atentados terroristas cometidos con bombas*

INSTRUMENTO RELATIVO A LA FINANCIACIÓN DEL TERRORISMO

IX. *1999 Convenio internacional para la represión de la financiación del terrorismo*

INSTRUMENTO ACERCA DEL TERRORISMO NUCLEAR

X. *Convenio internacional 2005 para la represión de los actos de terrorismo nuclear*

Subtema A: Lucha contra la guerra asimétrica en el siglo XXI.

Los subtemas son problemáticas propuestas por la mesa para promover la dinámica del debate. Si algún delegado considera que existe otra problemática basada en los temas preestablecidos relevante al comité, puede informarlo a la mesa con antelación, o proponerlo cuando la mesa abra una moción de agregar o suprimir subtemas durante el comité. Esto también aplica para remover alguno de los subtemas preestablecidos. Igualmente, agregar o remover subtemas solo se efectuara durante la moción establecida por la mesa, y por votación mayoritaria. (1/2+1)

Cuando existe un conflicto convencional hay dos ejércitos profesionales que básicamente tienen la misma experiencia, los mismos recursos, la misma tecnología y solo se diferencian en la ejecución de sus estrategias. A esto le llamamos **guerra simétrica**. La **guerra asimétrica** es cuando uno de los combatientes es un grupo más pequeño de insurgentes o rebeldes que utilizan tácticas no convencionales. Claramente las tácticas militares tradicionales utilizadas para luchar contra un ejército profesional ya no pueden funcionar.

Subtema B: Financiamiento de los grupos terroristas.

El financiamiento de los grupos terroristas fue descrito por el Centro de Transacciones Financieras y Análisis de Reporte de Canadá: **“El financiamiento del terrorismo proporciona fondos para la actividad terrorista. Puede involucrar fondos recaudados de fuentes legítimas, como donaciones personales y ganancias de empresas y organizaciones benéficas, así como de fuentes delictivas, como el tráfico de drogas, el contrabando de armas y otros bienes, el fraude, el secuestro y la extorsión.”**

Según el Convenio Internacional para la Represión de la Financiación del Terrorismo, aprobado por la Asamblea General de las Naciones Unidas en su resolución 54/109 el 9 de diciembre de 1999, si **"una persona comete un delito en el sentido del presente Convenio, si esa persona por cualquier medio, directa o indirectamente, ilícita y deliberadamente, proporciona o recauda fondos con la intención de que se utilicen o se tenga conocimiento de que se utilizarán, en su totalidad o en parte, para llevar a cabo un acto que constituya una ofensa o cualquier acto que tenga la intención de causar la muerte o lesiones corporales graves a un civil**”.

Posiciones de los Bloques

Poderes occidentales

Este bloque está formado por naciones que podrían caracterizarse como liberales e incluye los países de la Unión Europea, los Estados Unidos de América y sus aliados. Debido a sus puntos de vista similares, podrían considerarse como una coalición liderada por Estados Unidos.

Coalición Africana

La participación de la Unión Africana en esta cuestión es claramente evidente, ya que los países del África subsahariana se enfrentan a grandes ataques terroristas. La Unión Africana tendrá un papel clave en ser parte de la solución a este problema. También es esencial que los estados africanos se unan y cooperen para encontrar una solución.

Cooperación de Asia Oriental y el Pacífico

Los países de Asia oriental trabajan para debilitar la capacidad operativa de los grupos terroristas en la región. Estos países también "limitaron las actividades de las grandes organizaciones terroristas" en 2014.

Para concluir, es necesario resaltar el hecho de que los bloques antes mencionados son solo ejemplos de posibles coaliciones. Corresponde a los Estados ampliar y mejorar estos bloques, respetando sus políticas, pero siendo flexibles, como lo exigen las normas diplomáticas.

Preguntas Que Debe Resolver Una Resolución

1. ¿Qué métodos deben ser implementados por los ejércitos en la lucha contra la guerra asimétrica?
2. ¿Cuáles regulaciones internacionales deben ser modificadas o creadas para lograr resolver esta problemática?
3. ¿Cómo se puede prevenir que regulaciones futuras tengan un impacto negativo en la población civil?
4. ¿Cómo afectara el crecimiento de redes terroristas mundiales el desarrollo de la comunidad internacional?
5. ¿Qué mecanismos debe establecer la comunidad internacional para prevenir el financiamiento del terrorismo y que sanciones deben ser implementadas a quienes se encuentren culpables de este delito?

Tema B: Evolución de las Telecomunicaciones y la Información en el Contexto de la Seguridad Internacional

A medida que la tecnología avanza a pasos agigantados, se ha vuelto aún más importante asegurar la información privada y evitar que caiga en manos equivocadas. El desarrollo económico y la mejora de la seguridad tecnológica dependen del desarrollo de las telecomunicaciones y la tecnología de la información.
La tecnología en sí misma también puede presentar desafíos particulares a la formulación de políticas para hacer que los sistemas sean más seguros porque siempre están cambiando y desarrollándose con nuevas ramas que se exploran y metodologías más antiguas que se descartan.
Como ejemplo de lo anterior, la interceptación de información ha ayudado enormemente a los gobiernos a contrarrestar el crimen, pero también ha despertado preocupación sobre la legitimidad de tales búsquedas y la violación de la privacidad del público. A través de estos asuntos, la responsabilidad individual y la responsabilidad del Estado se han cuestionado impulsando a muchos países a mejorar sus capacidades de ciberseguridad.

Historia de la Problemática

En las últimas décadas, las autoridades nacionales y los gobiernos de todo el mundo han intentado explotar las tecnologías de la información y la comunicación (TIC) para mejorar las actividades gubernamentales y la comunicación con el pueblo. Aunque la adopción del gobierno electrónico ha mejorado en la mayoría de los Estados, la tasa de adopción exitosa varía de una nación a otra. En un corto período de tiempo, la tecnología de la información avanzó rápidamente desde los usos fundamentales de las TIC, como un medio para apoyar el trabajo administrativo, a la incorporación de las TIC a través de las acciones gubernamentales. Las Tecnologías de la Información y la Comunicación se refieren a los medios que brindan acceso a la información a través de las telecomunicaciones Estas tecnologías han traído grandes avances financieros y sociales y han ayudado al desarrollo de la sociedad.

Sin embargo, el desarrollo no regulado de las TIC y la rápida evolución tecnológica también pueden generar efectos indeseables. Debido a la naturaleza significativa de las redes de telecomunicaciones en la era de la globalización, las amenazas a la seguridad de la información se encuentran entre los desafíos más importantes para la sociedad moderna. Esto lleva a dos cuestiones importantes:

1. La explotación de las TIC como medio de imposición o como arma ofensiva
2. La necesidad de evitar el uso de dicha información por parte de grupos criminales o terroristas.

Las TIC pueden caracterizarse como un arma de doble filo, incluido el riesgo de utilizarlas para fines que van en contra de la paz y la seguridad internacional. Descuidar estos fenómenos podría resultar en el riesgo de la privacidad de las personas, las actividades comerciales de las empresas, las infraestructuras nacionales importantes y la información gubernamental clasificada.

Los terroristas pueden operar en el ciberespacio para destruir o controlar la información para sus propios objetivos. Los piratas informáticos entrenados pueden acceder a los bancos de dato, pueden robar o alterar información, o incluso

destruirla. Los objetivos de los terroristas pueden variar desde las instituciones financieras hasta las infraestructuras nucleares, sin mencionar los centros y sistemas de comunicación civil y militar.
En general, estos casos suelen estar relacionados con los siguientes sectores:

1. Comunicaciones, para comando y control, emisión de instrucciones / órdenes / instrucciones, etc.
2. Gestión de la percepción.
3. Reunión de inteligencia
4. Operaciones de apoyo financiero
5. Ataques cibernéticos

Por lo tanto, el uso indebido de las TIC conlleva importantes riesgos para la seguridad nacional e internacional, la seguridad pública y la estabilidad de la economía universal. Las medidas para fortalecer la seguridad de la información requieren una amplia colaboración internacional y sinergia para ser eficiente. El diálogo adicional, las soluciones factibles y factibles y la cooperación entre las naciones son indispensables para minimizar las amenazas y asegurar las infraestructuras nacionales y mundiales cruciales, para poder hacer frente a los desafíos a la seguridad de la información.

Tratados y resoluciones anteriores

1. El Grupos de Expertos Gubernamentales (GGE) informaron a la Asamblea General sobre desarrollos en telecomunicaciones en el contexto de la seguridad internacional, examinando las amenazas potenciales y existentes de la esfera cibernética y encontrando posibles medidas de cooperación para abordar ellos y emitió un informe en julio de 2010. El informe, entre otras cosas, recomienda **"Medidas de fomento de la confianza, estabilidad y reducción del riesgo para abordar las implicaciones del uso estatal de las TIC, incluidos los intercambios de opiniones nacionales sobre el uso de las TIC en los conflictos".** (2004)
2. El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) publicó una evaluación preliminar en 2012 sobre Ciberseguridad y Ciberguerra utilizando datos de fuente abierta, cómo los estados miembros de la ONU abordaron la ciberseguridad, ya sea que tengan un mando militar o una doctrina para tales actividades y si tienen un plan para adquirir capacidades cibernéticas ofensivas. Según este informe, solo 33 estados miembros incluyen la guerra cibernética en su planificación y organización militar. Además, la mayoría de los estados tienen graves deficiencias en los sistemas de infraestructura importantes que están en riesgo de ataque cibernético, incluidos el agua, la energía y los sistemas financieros.
3. Los equipos de respuesta a emergencias informáticas (CERT) están presentes en varios países que brindan servicios de seguridad al gobierno y sectores corporativos para proteger sus datos contra amenazas internas y externas y también prevenir, detectar y recuperar incidentes de seguridad informática.
4. El Convenio de la Federación de Rusia sobre Seguridad de la Información Internacional pretendía regular la actividad de los gobiernos para garantizar la seguridad de la información internacional y "actuar en contra del uso de la tecnología de la información y las comunicaciones para violar la paz y la seguridad internacionales" y "garantizar el libre intercambio de tecnología e información". al tiempo que se respeta la soberanía de los Estados y sus especificidades políticas, históricas y culturales existentes ".

Subtema A: Guerra Cibernética

Antes de empezar es necesario definir algunos aspectos.

- **Guerra Cibernética:** Una organización internacional o un actor no estatal se infiltra en los sistemas y redes informáticos de otra nación con el propósito de causar daños o interrupciones.
- **Ciberataque:** Una variedad de actividades realizadas a través del uso de la tecnología de la información y las comunicaciones.
- **Cyberterrorismo:** El uso intencional de actividades disruptivas, o la amenaza de las mismas, contra computadoras y/o redes, con el propósito de causar daño o más objetivos sociales, ideológicos, religiosos, políticos o similares, o intimidar a cualquier persona en apoyo de tales objetivos.
- **Delito Cibernético:** Cualquier violación no autorizada de la red y el robo de propiedad intelectual y otros archivos.

Todavía no existen criterios universales para determinar si un ciberataque es un acto delictivo o un acto de activismo, terrorismo o el uso de la fuerza de un estado comparable a un ataque armado. Por lo tanto, aún no se han establecido

órganos internacionales legalmente vinculantes para administrar explícitamente los asuntos transnacionales en el espacio cibernético. Existen dos definiciones para este término:

1. **Basado en los efectos**: El terrorismo cibernético existe cuando los ataques informáticos producen efectos lo suficientemente perturbadores como para generar un temor comparable al de un acto tradicional de terrorismo, incluso si es realizado por delincuentes.
2. **Basado en la intención:** el terrorismo cibernético existe cuando se realizan ataques informáticos ilegales o motivados políticamente para intimidar o coaccionar a un gobierno o pueblo para promover un objetivo político o causar un daño grave o un daño económico grave.

Esto nos lleva a la siguiente pregunta **¿Deberían incluirse las actividades cibernéticas en el Artículo 2.4 de la Carta de las Naciones Unidas como uso de la fuerza y en el derecho internacional consuetudinario?**

Usualmente, los ciber-terroristas pueden estar buscando una debilidad para explotar cualquier vulnerabilidad en infraestructuras cruciales. De hecho, los objetivos de un ciberataque consisten en las siguientes cuatro áreas:
• **Pérdida de integridad:** La información podría ser modificada incorrectamente
• **Pérdida de disponibilidad:** Los sistemas de información de misión crítica no están disponibles para los usuarios autorizados.
• **Pérdida de confidencialidad:** La información crítica se revela a usuarios no autorizados
• **Destrucción física:** Los sistemas de información crean daños físicos reales a través de comandos que causan fallas deliberadas.

Subtema B: Espionaje y Fugas de Información

El término espionaje puede interpretarse como el uso de espías, generalmente por parte de los gobiernos para obtener información política y militar. En términos generales, el espionaje electrónico está incluido en las llamadas Amenazas Persistentes Avanzadas (APT). Son un conjunto de procedimientos recurrentes de piratería informática, frecuentemente organizados por personas que apuntan a una entidad en particular y se considera una de las peores amenazas actuales, ya que concierne a estados, empresas y organizaciones.
Y aunque el espionaje electrónico aún no es tan común, puede describirse como una amenaza acelerada que no conoce fronteras nacionales. Además, los hackers usan múltiples formas que son intrínsecamente complicadas de detectar, y esto es exactamente lo que hace que el espionaje sea un arma eficiente.
Por lo tanto, está claro que la guerra de información ya no es un mito. En una economía inmaterial, los bienes digitales adquieren información o valor comercial y, a menudo, son de gran importancia. La desmaterialización facilita la acción a distancia, generalmente de países, donde se aplican marcos legales más indulgentes, y los peligros del castigo físico, gracias al anonimato, son limitados. La lucha contra las filtraciones de información demuestra la paradoja de la era digital. Una sociedad de la información puede convertirse fácilmente en una de riesgo.

Posiciones de Bloques

Poderes Occidentales: Estados Unidos tiene importantes capacidades de guerra cibernética; acusaciones recientes también han destacado su práctica controvertida de interceptar comunicaciones civiles (recopiladas de socios de la OTAN y otros aliados). Los aliados, incluidos el Reino Unido y Francia, tienen algunas de las capacidades más avanzadas de guerra cibernética, y han seguido el ejemplo de los Estados Unidos en la recopilación de información. Ver también las relaciones con China y Rusia a continuación.

China: Las relaciones entre los Estados Unidos y China se ven perjudicadas por sus desacuerdos sobre la tecnología de la información. Los departamentos gubernamentales de Estados Unidos identificaron al Ejército Popular de Liberación de China (ELP) como la fuente de ciberataques contra el gobierno de los EE. UU. Y las empresas privadas clave.

Rusia: Rusia copatrocinó una resolución para otorgarles a los estados un papel más importante en el gobierno del papel de Internet en una reunión de la Unión Internacional de Telecomunicaciones en abril de 2013, junto con China, Corea del Norte e Irán. Esto fue rechazado por los Estados Unidos y otros aliados de la OTAN causando algunas

fricciones. La decisión de Rusia de dar asilo a Edward Snowden también ha empeorado las relaciones con los Estados Unidos sobre cuestiones de ciberseguridad.

Latinoamerica: como una economía emergente de 'BRIC', Brasil se ha convertido en una especie de portavoz de las preocupaciones de los países en desarrollo cuando se trata de amenazas cibernéticas. La revelación de que Estados Unidos pudo haber llamado al teléfono de la presidenta brasileña Dilma Rousseff se enfureció en Brasil y en otras capitales mundiales, y se hicieron llamados para que los estados limiten sus actividades de recopilación de datos en línea o se arriesguen a incumplir las convenciones internacionales sobre objetivos adecuados de espionaje.

Irán: En 2010, Irán fue objeto de un ataque cibernético a gran escala conocido en Stuxnet que se dirigió a los activos de alto valor en el país, incluidas las instalaciones nucleares. El virus fue supuestamente creado por Israel y los Estados Unidos. En parte como respuesta, Irán ha afirmado desarrollar un potencial significativo de guerra cibernética.

Para concluir, es necesario resaltar el hecho de que los bloques antes mencionados son solo ejemplos de posibles coaliciones. Corresponde a los Estados ampliar y mejorar estos bloques, respetando sus políticas, pero siendo flexibles, como lo exigen las normas diplomáticas.

Preguntas Que Debe Resolver Una Resolución

- ¿Qué constituye un ciberataque, ciberespionaje y piratería informática? ¿Cómo deben responderse estas acciones? ¿Cuándo el uso de la tecnología de la información constituye un acto de agresión?
- ¿Qué principios pueden guiar un acuerdo internacional sobre las limitaciones del uso de la tecnología de la información en aras de mantener la paz y la seguridad internacionales?
- ¿Qué papel deberían tener los organismos existentes, como el Consejo de Seguridad de las Naciones Unidas, para determinar la responsabilidad de desestabilizar los ciberataques?
- ¿Cómo deberían responder los Estados miembros a la amenaza potencial de los actores no estatales que adquieren tecnología cibernética ofensiva?

Bibliografía

Matusitz, Jonathan Andre. “What Is Terrorism?” Terrorism & Communication: A Critical Introduction. Thousand Oaks, CA: SAGE, 2013

Laqueur, Walter (1987). The Age of Terrorism (2nd ed.). Boston: Little & Brown, p. 143.

Hoffman, Bruce (2006). Inside Terrorism (2nd ed.). New York: Columbia University Press, p. 43

League Convention (1937). Convention for the Prevention and Punishment of Terrorism. Article 1(2)

What is Terrorism Financing? http://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/terrorist-terroriste-eng.asp

Asymmetrical warfare. (2018). Retrieved from https://www.britannica.com/topic/asymmetrical-warfare

Los peligros de la guerra asimétrica | Nueva Sociedad. (2018). Retrieved from http://nuso.org/articulo/los-peligros-de-la-guerra-asimetrica/

Terrorism, Asymmetric Warfare And Nuclear Weapons. (2018). Retrieved from https://www.csis.org/analysis/terrorism-asymmetric-warfare-and-nuclear-weapons

Dion-Schwarz, C. (2018). Why It's So Hard to Stop a Cyberattack — and Even Harder to Fight Back. Retrieved from https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

¿Qué significa la declaración de "guerra cibernética" de Anonymous a Estado Islámico?. (2018). Retrieved from http://www.bbc.com/mundo/noticias/2015/11/151117_tecnologia_anonymous_estado_islamico_internet_ciberespacio_ciberataque_lb

Tvn, 2. (2018). Las diversas formas de espionaje cibernético de la CIA, según WikiLeaks. Retrieved from http://www.24horas.cl/internacional/las-diversas-formas-de-espionaje-cibernetico-de-la-cia-segun-wikileaks-2321973