COCMUN 2018

ONU - CS

CONSEJO DE SEGURIDAD DE LA ORGANIZACIÓN DE NACIONES UNIDAS



GUÍA DE ESTUDIO

AGENDA ABIERTA

- ARMAS AUTONOMAS
- INTELIGENCIA ARTIFICIAL
- CIBERSEGURIDAD
- ESPIONAJE INTERNACIONAL

MESA DIRECTIVA:

DANIELA REQUENA
LEONARDO MONSALVE
JOSE ARAUJO

CONSEJO DE SEGURIDAD

Al finalizar la Primera Guerra Mundial, surge por primera vez en la historia una organización política de carácter internacional en la que los países configurarían un nuevo orden mundial a través de herramientas diplomáticas no convencionales. El pionero de esta organización fue el ex presidente de los Estados Unidos de América, Woodrow Wilson, quien estableció una serie de principios claves que debía tener la organización. Ese documento se llama “Los 14 puntos de Wilson” que más adelante quedarían plasmados en el “Tratado de Versalles”.

Avanzando más en el tiempo, la Sociedad de Naciones discutió varios temas regionales como: la invasión a Manchuria, la Guerra del Chaco, la invasión a Abisinia, entre otros. Sin embargo, el declive de esta se originó motivado a la falta de pericia del Consejo de la organización, bien por sus procedimientos estrictos como por la imposibilidad de coerción y coacción realmente efectiva. El mayor de ellos era la aprobación de las decisiones por unanimidad. A medida que la Sociedad de Naciones iba sancionando a un Estado, éste se retiraba de la organización. En los últimos años de existencia quedaron 41 de 62 Estados que la conformaron en un inicio. Más tarde, al comenzar la segunda guerra mundial, se vio obligada a dejar de sesionar y desaparecer en su totalidad.

Durante 1939 – 1945 existieron varios documentos y reuniones, como la Declaración de St. James, la Carta del Atlántico, la Declaración de Moscú y la Declaración de Teherán, entre Franklin D. Roosevelt, Winston Churchill, Iósif Stalin, Charles de Gaulle y Chiang Kai-shek que establecieron los pilares para la Organización de Naciones Unidas (ONU). En cuanto se refiere al surgimiento del Consejo de Seguridad se pueden mencionar los siguientes:
Conferencia de Dumbarton Oaks y Yalta:

Fueron unas reuniones celebradas el 21 de agosto hasta el 7 de octubre de 1944 y del 4 al 11 de febrero de 1945 respectivamente. Los dirigentes de los cuatro países con mayor poder político y económico de la época (EEUU, URSS, Reino Unido y China) acordaron hacer un borrador de una organización internacional que cumpliera lo acordado en Moscú y Teherán que sería conocido posteriormente como la «Carta de las Naciones Unidas» en donde se creó una Asamblea General compuesta por todos los miembros de las Naciones Unidas encargado de estudiar, analizar y debatir cuestiones de cooperación internacional.

El Consejo de Seguridad compuesto por 5 miembros permanentes y 6 rotativos electos por la Asamblea General. Su rol fundamental sería el de mantener la

paz y seguridad internacional; el Consejo Económico y Social compuesto de 52 miembros rotativos que abordará temáticas vinculadas al desarrollo; la Corte Internacional de Justicia encargada de asistir en materia de derecho internacional a la organización y ser aquel organismo en donde los Estados podían litigar casos y; la Secretaría que sería el departamento logístico, administrativo, consultor y dirigente de esta organización.

Posteriormente en Yalta, las cuatro Potencias discutieron cuáles serían los métodos de trabajo y mecanismos de acción del Consejo de Seguridad estableciendo un sistema de votación donde los miembros permanentes poseían poder de veto. Además, acordaron que el Consejo de Seguridad debía tener a su disposición la posibilidad de recurrir a fuerzas armadas que estarían activas como contingentes e iban a ser suministradas por los miembros de la organización, en caso de ser necesario.

«Estamos decididos a establecer a la mayor brevedad posible, junto con nuestros aliados, una organización genera de carácter internacional para la conservación de la paz y la seguridad (...) Hemos convenido en que se debe convocar una conferencia de las Naciones Unidas en San Francisco, Estados Unidos, el 25 de abril de 1945, con el fin de redactar la carta de dicha organización sobre la base de las conversaciones oficiales de Dumbarton Oaks» -Declaración de Dumbarton Oaks.
Conferencia de San Francisco:

Fue una reunión celebrada desde el 25 de abril al 26 de junio de 1945, entre los 45 miembros de la Sociedad de Naciones y 4 países extra que invitó Charles de Gaulle para la reunión de los 51 fundadores de la Organización de Naciones Unidas (ONU). Fue la primera reunión en la que participaron una gran cantidad de gobiernos, tanto así que estos países representaban el 80% de la población mundial y se estimó que hubo un total de 3.500 participantes en la conferencia (asesores, delegados, logística, entre otros) más 2.500 personas que representaban a la prensa y medios de comunicación de todo el mundo.

La plenaria de la conferencia, fue la parte final de la reunión. Antes de eso, se organizaron un conjunto de comités preparatorios para establecer los principios y reglamentaciones de cada uno que luego serían sometidos ante ésta. Los comités preparatorios fueron enumerados y se encargaron de: i) Establecer los principios, normas, sistema de enmiendas a la Carta y la Secretaria de la ONU; ii) Cuestiones ligadas a la Asamblea General; iii) Cuestiones ligadas al Consejo de Seguridad; y iv) Cuestiones ligadas al Consejo Económico y Social y a la Corte Internacional de Justicia.

Cada comité preparatorio estaba dividido en doce comités técnicos y es gracias a este sistema que la Carta de las Naciones Unidas pudo ser hecha en dos

días, donde se simularon 400 sesiones de comités y 10 plenarias de la conferencia. Durante el proceso, muchas veces los Estados no se encontraban de acuerdo con lo que se disponía en la Carta, como el nuevo rol que se le dio a las organizaciones regionales en vista de que muchos países tenían acuerdos de defensa mutua. Otro tema discutido fue el derecho al veto, sobre este punto los países de menor tamaño precisaban que era una carga de responsabilidad y poder bastante desequilibrado y consideraban que impediría en muchas ocasiones el accionar del Consejo de forma objetiva. Sin embargo, se les concede dicho poder a los miembros permanentes debido a que se considera que a ellos les correspondía una carga mayor para el mantenimiento del nuevo orden mundial.

«La Carta de las Naciones Unidas que acabáis de firmar es una base sólida sobre la cual podremos crear un mundo mejor. La historia os honrará por ello. Entre la victoria en Europa y la victoria final, en la más destructora de todas las guerras, habéis ganado una batalla contra la guerra misma... Gracias a esta Carta, el mundo puede empezar a vislumbrar el día en que todos los hombres dignos podrán vivir libre y decorosamente» - Discurso de Truman al final de la Conferencia.

RESEÑA ACTUAL DEL COMITÉ

En la Carta de las Naciones Unidas se establecieron seis órganos principales en la Organización, incluido el Consejo de Seguridad. A fin de asegurar acción rápida y eficaz por parte de las Naciones Unidas, sus Miembros confieren al Consejo de Seguridad la responsabilidad primordial de mantener la paz y la seguridad internacionales, y reconocen que este actúa a nombre de ellos al desempeñar las funciones que le impone aquella responsabilidad, según lo establecido en el Artículo 24 de la Carta magna de la ONU.

El Consejo de Seguridad es el único órgano del sistema de las Naciones Unidas –y del mundo– de carácter coactivo y coercitivo, es decir, las decisiones tomadas en su seno no sólo son vinculantes dentro y fuera de las Naciones Unidas, sino que estas pueden imponerse obligatoriamente a quien o a quienes van dirigidas, exhortando coactivamente su cumplimiento y aplicando las medidas o sanciones a que haya lugar en caso de inobservancia de sus decisiones.

El Consejo de Seguridad está compuesto por:

a) Miembros Permanentes; Son Miembros que siempre han estado en este consejo desde su nacimiento e instalación, gozan de Derecho a voto y además poseen el Derecho a Veto, es decir, cualquiera de estos al votar en contra de una Posible Resolución esta se desaprueba automáticamente aun así hubiere sido aprobada por la

Mayoría de miembros. El fundamento de esta modalidad no aparece explícitamente en la Carta de las Naciones Unidas, el hecho de que una decisión sustantiva requiere de un consenso de todos los miembros permanente, se entiende que cualquiera la puede desaprobar. Estos Miembros son:

1. Estados Unidos de América
2. República Francesa
3. República Popular China (antes República de China)
4. Reino Unido de Gran Bretaña e Irlanda del Norte
5. Federación Rusa (Antes Unión de Repúblicas Socialistas Soviéticas)

b) Miembros No Permanentes: Son Miembros que son elegidos por la Asamblea General que obedecen a una distribución Geográfica Equitativa, gozan de Derecho a voz y voto, los Miembros No Permanentes son:

1. Perú (en representación de América Latina y el Caribe)
2. Bolivia (en representación de América Latina y el Caribe)
3. Guinea Ecuatorial (en representación de África)
4. Etiopia (en representación de África)
5. Costa de Marfil (en representación de África)
6. Kuwait (en representación de Asia)
7. Kazajistán (en representación de Asia)
8. Países Bajos (en representación de Europa Occidental y Otros Estados)
9. Suecia (en representación de Europa Occidental y Otros Estados)
10. Polonia (en representación de Europa Oriental).

Recordando que siempre debe ser Miembro un País Árabe, bien sea africano o asiático.

Un Estado que es Miembro de las Naciones Unidas, pero no del Consejo de Seguridad podrá participar sin derecho a voto, en sus deliberaciones cuando el Consejo considera que los intereses de ese país se ven afectados. Tanto los miembros y los no miembros de las Naciones Unidas, si son partes en una controversia que se considera por el Consejo, podrán invitarse a participar, sin derecho a voto en las deliberaciones del Consejo, el Consejo establece las condiciones para la participación de un Estado no miembro. En el caso de este comité, fueron invitados a este Consejo:

- Irán
- Turquía
- Brasil
- México
- Alemania

- Japón
- India
- Israel
- Corea del Sur

Facultades y obligaciones:

1. Mantener la paz y la seguridad internacionales de conformidad con los propósitos y principios de las Naciones Unidas;
2. Investigar toda controversia o situación que pueda crear fricción internacional;
3. Recomendar métodos de ajuste de tales controversias, o condiciones de arreglo;
4. Elaborar planes para el establecimiento de un sistema que reglamente los armamentos;
5. Determinar si existe una amenaza a la paz o un acto de agresión y recomendar qué medidas se deben adoptar;
6. Instar a los Miembros a que apliquen sanciones económicas y otras medidas que entrañan el uso de la fuerza, con el fin de impedir o detener la agresión;
7. Emprender acción militar contra un agresor;
8. Recomendar el ingreso de nuevos Miembros;
9. Ejercer las funciones de administración fiduciaria de las Naciones Unidas en "zonas estratégicas";
10. Recomendar a la Asamblea General la designación del Secretario General y, junto con la Asamblea, elegir a los magisterios de la Corte Internacional de Justicia.

Órganos Subsidiarios del consejo de seguridad:

1. Comité de Estado Mayor:

El Comité de Estado Mayor ayuda a planificar las medidas de naturaleza militar que adoptan las Naciones Unidas y a regular los armamentos.

2. Comités de sanciones (especiales):

La finalidad de las sanciones obligatorias es ejercer presión sobre un Estado o entidad para que respete los objetivos fijados por el Consejo de Seguridad sin recurrir al uso de la fuerza. Para el Consejo de Seguridad, las sanciones son pues un instrumento importante para hacer cumplir sus decisiones. Debido al carácter universal de las Naciones Unidas, el Consejo es un órgano especialmente apropiado para establecer y supervisar medidas de este tipo.

El Consejo ha utilizado las sanciones obligatorias como instrumento para hacer respetar sus decisiones cuando se ha puesto en peligro la paz y ha fracasado la vía diplomática. Hay sanciones generales de tipo económico y comercial, y

otras más específicas, como el embargo de armas, la prohibición de viajar, las restricciones financieras o diplomáticas, entre otras.

3. Comités permanentes y órganos especiales:

Los comités permanentes tienen una composición abierta y, en general, se constituyeron para tratar ciertas cuestiones de procedimiento, como la admisión de nuevos miembros. Los comités especiales se establecen por tiempo determinado y se encargan de cuestiones específicas.

4. Operaciones de Mantenimiento de Paz y Misiones Políticas:

En las operaciones de mantenimiento de la paz participa personal militar, civil y de policía, que trabaja para proporcionar seguridad, prestar apoyo político y para la consolidación de la paz. Estas operaciones son flexibles y en las dos últimas décadas han adoptado distintas formas. Las operaciones de mantenimiento de la paz multidimensionales que se despliegan en la actualidad se destinan no solo a mantener la paz y la seguridad, sino también a facilitar los procesos políticos, proteger a la población civil, prestar asistencia para el desarme, desmovilización y reintegración de excombatientes, apoyar la organización de procesos electorales, proteger y fomentar los derechos humanos, y ayudar a restablecer el estado de derecho.

Las misiones políticas son parte del conjunto de operaciones de paz de las Naciones Unidas que se desarrollan en distintas etapas del ciclo de los conflictos. En algunos casos, tras la firma de un acuerdo de paz, las misiones políticas supervisadas por el Departamento de Asuntos Políticos durante la fase de negociaciones han sido sustituidas por misiones de mantenimiento de la paz. En otros casos, las operaciones de mantenimiento de la paz de las Naciones Unidas han dejado paso a misiones políticas especiales que dirigen actividades de consolidación de la paz a más largo plazo.

5. Comisión de consolidación de la Paz

Es un órgano consultivo intergubernamental que apoya iniciativas en pro de la paz en países que acaban de salir de un conflicto y es un complemento fundamental para la capacidad de la comunidad internacional en la agenda global de la paz.

La Comisión de Consolidación de la Paz desempeña un papel singular al:

- Reunir a todos los agentes pertinentes, incluidos los donantes internacionales, las instituciones financieras internacionales, los gobiernos nacionales, los países que aportan contingentes;
- Conseguir recursos; y

- Prestar asesoramiento sobre estrategias integrales de consolidación de la paz y recuperación después de los conflictos y proponer esas estrategias y, cuando procede, poner de relieve cualquier insuficiencia que amenace con perturbar la paz.

6. Cortes y Tribunales Internacionales.

Establecidas para gestionar casos especiales de agresión a la humanidad en el territorio de la Ex Yugoslavia y la Republica de Ruanda.

Funcionamiento y Mandato:

Para un mejor funcionamiento del Consejo, la Carta de las Naciones Unidas y el Reglamento Provisional en sus artículos 28 y 29 respectivamente, le dan la facultad de establecer al Consejo de Seguridad, todos los comités y organismos subsidiarios que considere necesarios para el desempeño de sus funciones que ayuden al mantenimiento de la paz y seguridad internacional.

El período de sesiones del Consejo de Seguridad es constante, es decir, cada vez que surja una controversia que ponga en flagelo la paz y la seguridad internacional, el Consejo se podrá reunir. Incluso sin la existencia de un problema internacional, el Consejo puede discutir cuestiones generales que consideren que pueda afectar a la comunidad internacional. El Consejo puede emanar distintos documentos para la resolución de una controversia, como bien los son; las resoluciones, declaraciones de presidencia, notas de la presidencia, carta de la presidencia y comunicados de prensa.

El Consejo de Seguridad es el principal órgano garante de mantener la paz y seguridad internacionales dentro de las Naciones Unidas. Su jurisdicción se encuentra contemplada en la Carta de las Naciones Unidas en los capítulos VI, VII, VIII y XII.

CAPÍTULO VI: ARREGLO PACÍFICO DE CONTROVERSIAS:

El artículo 33 permite al Consejo de Seguridad resolver, ante todo, cualquier controversia «mediante: la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección.»

Del mismo modo, cualquier Estado Miembro, o no del Consejo, puede investigar cualquier situación susceptible a un conflicto internacional y llevarlo al debate de este órgano. También podrá recomendar el procedimiento de ajuste de controversias que ellos determinen. En el caso de controversias de

orden jurídico deberá ser sometido a la Corte Internacional de Justicia según lo dispuesto en el Estatuto.

CAPÍTULO VII: ACCIÓN EN CASO DE AMENAZAS A LA PAZ, QUEBRANTAMIENTOS DE LA PAZ O ACTOS DE AGRESIÓN:

El Consejo de Seguridad puede determinar un caso que amenace a la paz y seguridad internacional, que no pueda ser resuelto por los mecanismos del Capítulo VI de la Carta, y someterlo a debate dentro del mismo seno para tomar una medida coercitiva. Las medidas coercitivas estipuladas en los artículos 41 y 42 de la Carta son:

- Sin uso de la fuerza: Interrupciones de las actividades comerciales, económicas y de los medios de comunicación y/o; ruptura de las relaciones diplomáticas;
- Uso de la fuerza: Pueden usar recursos militares aéreos, marítimos o terrestres para cualquier tipo de operación.

Asimismo, cuando el Consejo de Seguridad determinase el uso de la fuerza para la resolución de un conflicto, en primer lugar, según el artículo 44 de la Carta, el Consejo invitará a aquel Miembro que no esté representado dentro de la reunión a participar de las decisiones relativas al empleo de las contingentes de las fuerzas armadas de dicho miembro. Los Estados Miembros de Naciones Unidas tienen el deber de aportar dichos contingentes, los cuales deben estar listos para cuando se soliciten según lo establecido en el artículo 45 de la Carta, que reza que «a fin de que la Organización pueda tomar medidas militares urgentes, sus miembros mantendrán contingentes de fuerzas aéreas nacionales inmediatamente disponibles para la ejecución (...)».

CAPÍTULO VIII: ACUERDOS REGIONALES:

Antes del establecimiento de Naciones Unidas, existían organismos regionales para la resolución de conflictos. Con respecto a estos, el Consejo de Seguridad debe trabajar en cooperación, siempre y cuando se respeten los principios de la Carta. La labor de los organismos regionales será una diplomacia preventiva, sin embargo, no está limitada a ella y evitar que estalle un conflicto y el establecimiento de la paz para evitar que se prolonguen los mismos. Es importante resaltar que los organismos regionales no pueden aplicar medidas coercitivas sin previo permiso del Consejo de Seguridad y estos deberán informar al Consejo sobre todas las acciones que han tomado para poder hacer una labor efectiva.

SEGURIDAD INTERNACIOANL FRENTE AL DESARROLLO TECNOLOGICO

El hombre y su evolución, han estado marcados por una constante serie de cambios, bien sean graduales o violentos, los mismos están determinados por una inherente transformación. Su condición social ha sido la que le ha hecho abordar la dicotomía “ellos-nosotros”, con la cual tras milenios sentó las bases de los Estados-Nación modernos y el Derecho Internacional desde 1648 hasta nuestros días, cuya cristalización se dio definitivamente en 1945 bajo la creación de la Organización de las Naciones Unidas.

Sin embargo, el abordaje de las relaciones de grupos humanos bajo esta dicotomía bien se ha dado bajo medios pacíficos o en términos de convivencia, no es menos cierto que también se ha fundamentado dentro de un clima de conflictividad, las guerras han marcado plenamente la evolución del hombre y sus normas de convivencia al punto que es precisamente con el cese del conflicto bélico de mayor escala registrado hasta nuestros días (La Segunda Guerra Mundial, período histórico comprendido entre 1939-1945) fue el punto determinante para la reestructuración de las relaciones, no solo entre grupos humanos (bajo el enfoque de los derechos humanos universales) sino también desde los Estados-Nación bajo las normas de la diplomacia y el Derecho Internacional Público sobre unas premisas comunes, que no han sido otras que “preservar la paz y seguridad internacional”.

Otro elemento que ha sido determinante a la hora de abordar las relaciones humanas a lo largo de la historia, ha sido, eminentemente, el desarrollo tecnológico, un desarrollo que nace no solo para la subsistencia del hombre sino también para superar las adversidades que se le presentan en su devenir, lo que en términos reales viene a ser la materialización o puesta en práctica de su inteligencia. En tal sentido, el desarrollo tecnológico como motor del progreso ha hecho capaz no solo de brindar mayor bienestar a la humanidad, sino a incluso borrar las barreras físicas entre los individuos, siendo sus efectos más contrastables justo en esta era; la era de la globalización, donde desde décadas atrás se habla de “humanidad” por encima de “nacionalidades”, siendo así, que el mundo de hoy y del mañana está en plena interconexión brindando múltiples ventajas y oportunidades al interés general, pero también despertando nuevas amenazas.

En lo que nos respecta, podemos definir la seguridad internacional (en términos negativos) como la ausencia de conflictos entre naciones o dentro de las naciones que afecten al resto, lo que viene a ser la ausencia de guerras y/o conflictos de diversa índole como el terrorismo. En ese sentido, desde 1945 se

ha hecho preponderante para los Estados Miembros de las NN.UU la consecución de este fin conjunto al de la paz, cuyo medio más idóneo a la luz de la Carta de las Naciones Unidas, ha sido la creación del Consejo de Seguridad, siendo que a través de este se alberga la toma de decisiones de mayor peso en el planeta sobre estos aspectos ya mencionados.

Sin embargo, podemos decir que como el hombre y la tecnología avanzan, las formas de hacer guerra también avanzan al mismo paso. Lind (1989) afirmó que en la historia universal, la guerra ha tenido cuatro estadios o generaciones; la **Primera Generación**, consiste en aquellos conflictos en los que se hacía uso de armas de fuego por parte de cuerpos armados profesionales que desembocaron en la industrialización de la guerra, dando paso a la **Segunda Generación**, donde el conflicto resalta por las grandes movilizaciones de tropas y de maquinaria, así como la creación de nuevos medios de defensa como las guerras de desgaste, que irremediablemente condujo a nuevos planteamientos tácticos que dieron paso la **Tercera Generación** donde toman rol protagónico la mecanización de los cuerpos armados, el factor sorpresa, la búsqueda de superioridad en materia tecnológica, logística y comunicacional que llega a tal punto, que resulta necesario para los diversos factores beligerantes posteriores a 1945 contrarrestar los grandes poderes militares con estrategias basadas en el mismo factor sorpresa, dando paso a la **Cuarta Generación**, que se basa en el empleo de técnicas no convencionales como el terrorismo, las guerras de guerrillas, guerras asimétricas, la propaganda y muy recientemente, la guerra comercial, siendo todas estas la suma de técnicas que no se basan en atacar a los ejércitos o a los Estados-Nación, sino a sus poblaciones desde células que afectan los estamentos del Estado desde el orden público, la cibernética y la Política.

ARMAS AUTONOMAS

La revolución robótica está siendo descrita por muchos como la siguiente gran revolución en cuestiones militares, de una importancia equivalente a la introducción de la pólvora y las bombas nucleares, lo cual supone una catálogo de dilemas jurídicos, políticos, morales y éticos que deben ser explorados.

La revisión de las cuestiones clave planteadas por los sistemas autónomos de armas en virtud del Derecho Internacional Humanitario (DIH), basándose en los documentos publicados anteriormente del Comité Internacional de la Cruz Roja (CICR)

A los fines de este análisis, se utiliza un sistema autónomo de armas definido de la siguiente manera:

Cualquier sistema de armas con autonomía en sus funciones críticas, es decir, un sistema de armamento que puede seleccionar (buscar, detectar, identificar, rastrear o seleccionar) y atacar (usar fuerza contra, neutralizar, dañar o destruir) objetivos sin Intervención humana.

Después del lanzamiento inicial o la activación por parte de un operador humano, es el sistema de arma en sí, que utiliza sus sensores, programación de computadora (software) y armamento, que asume las funciones de selección que de otro modo serían controladas por humanos.

Esta definición de trabajo abarca cualquier sistema de armas que pueda seleccionar y atacar objetivos de forma independiente, incluidas algunas armas existentes y posibles sistemas futuros. La definición proporciona una base útil para un análisis legal al delinear el amplio alcance de la discusión sobre los sistemas autónomos de armas sin la necesidad de identificar inmediatamente los sistemas que plantean problemas legales.

En ese sentido, la definición no pretende prejuzgar el nivel de autonomía en los sistemas de armas que pueden o no considerarse lícitos. Por el contrario, el CICR ha propuesto que los Estados determinen dónde deben colocarse estos límites evaluando el tipo y grado de control humano requerido en el uso de sistemas de armas para realizar ataques, como mínimo, para cumplir con el DIH y, además, para satisfacer las consideraciones éticas

Si bien el DIH crea obligaciones para los Estados y las partes en los conflictos armados, las normas del DIH son en última instancia implementadas por sujetos humanos que son responsables de cumplir con estas normas en la realización de ataques, y deben rendir cuentas por las violaciones.

Los motivadores principales para el uso de sistemas autónomos, robóticos o no tripulados en el campo de batalla incluyen los siguientes:

- Multiplicación de fuerza. Con los robots, se necesitan menos soldados para una misión determinada y un soldado individual ahora puede hacer el trabajo de muchos.
- Expandiendo el espacio de batalla. Los robots permiten el combate en áreas más grandes de lo que era posible anteriormente.
- Extendiendo el alcance del combatiente. La robótica permite a un soldado individual llegar más lejos en el espacio de batalla al, por ejemplo, ver o golpear más lejos.
- Reducción de bajas. Los robots permiten retirar a los soldados de las misiones más peligrosas y que amenazan potencialmente la vida de los mismos.

I. Cumplimiento del Derecho Internacional Humanitario

Los sistemas de armas autónomas, tal como se definen, no están específicamente regulados por los tratados de DIH; sin embargo, es indiscutible que cualquier sistema autónomo de armas puede y debe ser utilizado de conformidad con el DIH.

La responsabilidad de garantizar esto recae, ante todo, en cada Estado que desarrolla, despliega y usa armas; mientras que los temas principales del DIH son las partes en un conflicto armado, las normas sobre la conducción de las hostilidades -en particular las reglas de distinción, proporcionalidad y precauciones en el ataque están dirigidas a aquellos que planean, la decisión y llevar a cabo un ataque.

Estas reglas de DIH crean obligaciones para los combatientes humanos en el uso de armas para llevar a cabo ataques, sin embargo, esta responsabilidad, no se pueden transferir a una máquina, programa de computadora o sistema de armas. De ello se desprende que un sistema autónomo de armas planteará problemas si impide que los comandantes u operadores hagan estos juicios legales.

III. Los "principios de la humanidad" y los "dictados de la conciencia pública"

Se mencionan especialmente en el artículo 1 del Protocolo adicional I y en el preámbulo del Protocolo adicional II de los Convenios de Ginebra, denominado Cláusula Martens y proporciona un vínculo entre las consideraciones éticas y el DIH; Establece que, en los casos no cubiertos por los tratados existentes, los civiles y los combatientes permanecen protegidos por el DIH consuetudinario, los principios de la humanidad y los dictados de la conciencia pública.

Los principios de la humanidad son un punto de referencia universal, que evita la suposición de que todo lo que no está explícitamente prohibido está permitido.

Con respecto a la conciencia pública, hay una sensación de profunda incomodidad con la idea de cualquier sistema de armas que coloque el uso de la fuerza más allá del control humano.

II. Revisión legal de nuevas armas

La obligación de llevar a cabo revisiones legales de nuevas armas en virtud del artículo 36 del Protocolo adicional I de los Convenios de Ginebra es importante para garantizar que las fuerzas armadas de un Estado sean capaces de conducir hostilidades de conformidad con sus obligaciones internacionales.

La revisión legal debe exigir un nivel muy alto de confianza que una vez activado, el sistema autónomo de armas funcionaría de manera predecible y confiable según lo previsto. Esto plantea desafíos únicos para garantizar que la previsibilidad y la confiabilidad se prueban y verifican para todos los escenarios de uso previsibles.

Existe un acuerdo general entre los Estados Parte de la Convención sobre Ciertas Armas Convencionales (CCW) de que el control humano "significativo" o "efectivo", o "niveles apropiados de juicio humano" deben mantenerse sobre los sistemas de armas y el uso de la fuerza

Por su parte, el CICR ha pedido que se mantenga el control humano sobre los sistemas de armas y el uso de la fuerza para satisfacer los requisitos legales y éticos. Un cierto nivel de control o participación humana (incluso traduciendo la intención del usuario en el funcionamiento del sistema de armas) es inherente a la implementación de las reglas del DIH sobre la conducción de las hostilidades.

Para sistemas autónomos de armas, el control ejercido por humanos puede tomar diversas formas y grados en diferentes etapas de desarrollo, despliegue y uso, incluyendo los siguientes:

1- Etapa de desarrollo

El control humano puede ejercerse en la etapa de desarrollo, incluso mediante el diseño técnico y la programación del sistema de armamento que debe garantizar que el sistema de armas se pueda utilizar de conformidad con el DIH y otras leyes internacionales aplicables en las circunstancias previstas o previstas de uso. Los parámetros operacionales sobre el uso del arma deben integrarse en las instrucciones militares para su uso, por ejemplo, limitar su uso a una situación específica, restringir su movimiento en el tiempo y el espacio, o permitir la supervisión humana.

2- Etapa de activación

En este punto, que implica la decisión del comandante u operador de usar un sistema de arma particular para un propósito particular, ya sea en un ataque específico, o para responder a una amenaza general durante un período de tiempo específico, esta decisión por parte del comandante u operador debe basarse en el conocimiento y la comprensión suficientes del funcionamiento del arma en las circunstancias dadas para garantizar que operará según lo previsto y de conformidad con el DIH.

Este conocimiento debe incluir una conciencia situacional adecuada del entorno operacional, especialmente en relación con los riesgos potenciales para los civiles y los objetos civiles.

3- Etapa de operación

El riesgo de violación de DIH se puede reducir manipulando estos parámetros operativos hasta el punto de activación; sin embargo, para garantizar el cumplimiento del DIH, puede ser necesario un control humano adicional durante la etapa de operación, cuando el arma selecciona y ataca objetivos de forma autónoma. El nivel de supervisión humana y la capacidad de intervenir

después de la activación, proporciona un medio por el cual se puede ejercer un mayor control sobre un ataque.
Cuando el rendimiento técnico del arma y los parámetros operacionales establecidos durante las etapas de desarrollo y activación sean insuficientes para garantizar el cumplimiento del DIH en la realización de un ataque, será necesario conservar la capacidad de control humano y de toma de decisiones durante la etapa de operación.

III. Responsabilidad por violaciones del DIH

Se han formulado preguntas sobre si el uso de sistemas autónomos de armas puede conducir a una "brecha de rendición de cuentas" legal en caso de violaciones del DIH. Si bien siempre habrá un humano involucrado en la decisión de desplegar y activar un arma a la que se pueda atribuir responsabilidad, la naturaleza de la autonomía en los sistemas de armas significa que las líneas de responsabilidad pueden no siempre ser claras.

En virtud del derecho internacional general que rige la responsabilidad de los Estados, se los consideraría responsables de actos internacionalmente ilícitos, como violaciones del DIH cometidas por sus fuerzas armadas utilizando un sistema autónomo de armas.
Según el DIH y el derecho penal internacional, los límites del control humano sobre un sistema autónomo de armas podrían dificultar la identificación de personas involucradas en la programación. Los seres humanos que han programado o activado los sistemas de armas pueden no tener el conocimiento o la intención necesarios para ser considerados responsables, debido al hecho de que la máquina, una vez activada, puede seleccionar y atacar objetivos de forma independiente.
Los programadores pueden no tener conocimiento de las situaciones concretas en las que, en una etapa posterior, se podría desplegar el sistema de armas y en el cual podrían ocurrir violaciones al DIH y, en el momento de la activación, los comandantes pueden desconocer la hora exacta y el lugar donde se produjo el ataque, tendría lugar.
Por otro lado, un programador que programa intencionalmente un arma autónoma para operar en violación del DIH o un comandante que activa un arma que es incapaz de funcionar legalmente en ese entorno sería penalmente responsable de una violación resultante. Además, bajo las leyes de responsabilidad por productos defectuosos, los fabricantes y programadores también podrían ser responsables de los errores en la programación o del mal funcionamiento de un sistema autónomo de armas.

IV Armas autónomas y estabilidad
Durante la guerra fría, el concepto de "estabilidad" surgió como un factor importante en la evaluación de nuevas tecnologías de arma. Se observó la

estabilidad como algo bueno, porque significaba mantener el status quo: paz. La inestabilidad fue vista como peligrosa, porque podría llevar a la guerra. Hay varias variantes de este concepto. La inestabilidad del primer golpe se refiere a la idea de que algunas armas o posturas de despliegue pueden dar ventaja a cualquier lado que golpee primero, incentivando así a las naciones a lanzar un ataque preventivo en una crisis. Una situación estable es aquella en la que ningún lado puede obtener una ventaja golpeando primero.

Un concepto relacionado es la estabilidad de la crisis, que se ocupa de evitar la escalada a través de errores de cálculo, accidentes o falta de control efectivo sobre las fuerzas militares. Las falsas alarmas, los malentendidos y la niebla de la guerra a menudo contribuyen a la inestabilidad en las crisis.
Los protocolos de seguridad que reducen el riesgo de accidentes y aumentan el control de los líderes nacionales sobre sus propias fuerzas pueden aumentar la estabilidad; del mismo modo, las medidas que aumentan la comunicación y la transparencia entre las naciones, como las líneas directas de crisis, pueden aumentar la estabilidad.

1. Control humano sobre la guerra

Debido a que la esencia de las armas autónomas es que los humanos han delegado la toma de decisiones de fuerza letal en la máquina, una pregunta es si las armas autónomas aumentarían o disminuirían el control humano en la guerra.
Si las armas autónomas llevaran a un mayor control humano sobre la iniciación de la guerra, la escalada y la terminación, entonces sería deseable. Un mayor control se estabilizaría; haría menos probable los accidentes y los errores de cálculo. Si las armas autónomas llevaran a un menor control humano, entonces eso podría aumentar el riesgo de una escalada involuntaria y sería indeseable.

Podría parecer contra-intuitivo que la autonomía podría aumentar el control humano, sin embargo una forma en que las armas autónomas podrían potencialmente aumentar la estabilidad sería aumentar el control de los líderes nacionales sobre cómo se comportan sus fuerzas en las crisis; Las personas pueden desviarse de las órdenes, los sistemas autónomos, en teoría, harán exactamente lo que están programados para hacer.

2. El valor del juicio humano en crisis

Desafortunadamente, los sistemas autónomos tienen una gran debilidad: son inflexibles pues si el contexto para su acción cambia, a menudo carecen de la flexibilidad para adaptarse, esto representa un problema importante para controlar la escalada.
Hay muchos ejemplos de humanos que usan su juicio para evitar la escalada en las crisis. En 1983, el teniente coronel soviético Stanislav Petrov ignoró la información de los satélites de alerta temprana de que Estados Unidos había

lanzado un ataque sorpresa porque la información no se ajustaba al contexto más amplio. Más tarde dijo sobre la advertencia de misiles: "Tenía un presentimiento extraño".

Las armas autónomas eliminarían el potencial del juicio humano para considerar el contexto específico de una acción, los militares tienen un concepto de "intención del comandante"; Los subordinados deben entender no solo sus órdenes, sino también el resultado que su comandante pretende lograr.

Es decir, los humanos tienen la capacidad de imaginar lo que sus líderes querrían, dada la situación en la que se encuentran; esto permite a los humanos desviarse de sus instrucciones si es necesario para cumplir con la intención de su liderazgo.

3. Controlar la escalada y la terminación de la guerra

Los accidentes, en el pasado, llevaron a intercambios de ojo por ojo que resultaron en conflictos que escalaron a niveles de destrucción que ambos lados consideraron indeseables. Tanto los humanos como las máquinas pueden causar accidentes, pero la autonomía permite la operación a mayor escala, lo que puede aumentar las consecuencias de los accidentes. Un arma autónoma que funciona mal o es atacada puede seguir atacando a los objetivos equivocados hasta que se quede sin munición. Además, dado que el mismo software se replicaría en otras armas autónomas del mismo tipo, muchos sistemas podrían fallar al mismo tiempo, lo que provocaría accidentes a gran escala; incluso si los humanos finalmente recuperaran el control de dichos sistemas, sería casi imposible disminuir las tensiones si las armas autónomas hubieran causado una destrucción significativa.

La terminación de la guerra también podría ser una preocupación si las armas autónomas estuvieran operando por largos períodos de tiempo sin enlaces de comunicación con los controladores humanos, como el submarino, donde las comunicaciones son un desafío.

4. El ritmo de la batalla

Incluso si no hubiera accidentes con armas autónomas, podrían socavar la estabilidad si aceleran el ritmo de la batalla más allá de los tiempos de reacción humana. La autonomía ya es utilizada por más de 30 naciones para defenderse contra los ataques con cohetes y misiles que podrían abrumar a los operadores humanos. Cuando se utilizan puramente en un contexto defensivo, estas aplicaciones de la autonomía probablemente aumentarían la estabilidad, ya que hacen más difícil para un adversario obtener una ventaja al golpear primero. Sin embargo, si ambas partes usaran armas autónomas ofensivamente, el resultado podría ser una "singularidad" militar, donde la velocidad de la acción en el campo de batalla eclipsaría la velocidad de la toma de decisiones humana. Esto podría socavar la estabilidad si los líderes nacionales pierden la capacidad de controlar efectivamente un conflicto, es decir, si aceleraran la velocidad de la guerra, no proporciona a los humanos

tiempo para considerar sus acciones, lo que se traduce en guerras más duraderas y destructivas.

5. Posibles enfoques de control de armas

Las armas autónomas no son la primera nueva tecnología militar con la que la humanidad ha lidiado. Las prohibiciones sobre las armas se remontan a la antigüedad. Existen muchos ejemplos de éxitos y fracasos en el control de armamentos a lo largo de la historia. Los siguientes ejemplos apuntan a varios temas comunes.

Cuando los países se abstienen de construir armas, lo hacen por razones estratégicas, no simplemente porque las armas están prohibidas. Los tratados comunican qué armas las naciones creen que son inaceptables. Sin embargo, a menudo estas han violado tratados en la guerra, al mismo tiempo; las naciones a veces se han abstenido de desplegar o usar ciertas armas aun sin tratados formales por miedo a la reciprocidad.

Los regímenes de no proliferación pretenden limitar el acceso a tecnologías peligrosas. Algunos tratados prohíben la producción y el almacenamiento de ciertas armas. Los tratados de limitación de armas limitan las cantidades de ciertas armas que las naciones pueden poseer en tiempos de paz; mientras que algunos tratados permiten que las armas sean utilizadas en algunas circunstancias en la guerra, pero no en otros

La restricción mutua es imposible sin claridad sobre qué armas o métodos de guerra están prohibidos, los tratados que se centran en la intención detrás del arma tienen la mejor trayectoria de éxito; aquellos tratados con definiciones muy detalladas han tenido cierto éxito, mientras que las reglas complicadas sobre cómo se pueden usar las armas en tiempo de guerra -permitiendo algunos usos pero no otros- han tenido menos éxito.

Un factor importante en la probabilidad de éxito de una prohibición propuesta es el equilibrio entre la percepción del daño causado y su valor militar percibido, muchas armas que han sido prohibidas con éxito solo tienen un valor militar marginal pero pueden causar un gran sufrimiento o se las considera desestabilizadoras; con respecto a esto las prohibiciones o regulaciones preventivas tienen ciertos desafíos únicos.

Por un lado, puede ser más fácil prohibir armas de las que los países aún no dependen para su defensa; por otro lado, el hecho de que el arma aún no exista puede significar que la percepción del daño causado y su valor militar. están en cuestión.

Otro desafío es lograr una definición que supere la prueba del tiempo a medida que la tecnología evoluciona.

Incluso los tratados más exitosos no tienen un cumplimiento del 100%. Particularmente si la tecnología para construir un arma prohibida está ampliamente disponible, es probable que algunos terroristas o naciones deshonestas los construyan, independientemente del grado de condena internacional.

Los regímenes de verificación formal no son necesariamente indispensables para el éxito, pero la transparencia sí lo es (particularmente si se considera que un arma es valiosa, las naciones querrán saber que los posibles adversarios no están haciendo trampa) algunos tratados tienen regímenes de verificación formal con inspecciones para garantizar que todas las partes se adhieren a un tratado.
La verificación formal y las inspecciones pueden no ser necesarias si las naciones pueden observar el cumplimiento de los demás a distancia, por ejemplo, mediante el uso de satélites. La transparencia es este caso es un gran desafío si la diferencia entre un arma prohibida y una permitida está en el software, que no es observable desde el exterior.

PREGUNTAS CLAVES

1. ¿Las obligaciones legales básicas para un comandante u operador en el uso de sistemas de armas se extienden a la operación con armas autónomas?

2. Si bien las reglas DIH crean obligaciones para los combatientes humanos en el uso de armas, en el caso de ataques perpetrados con armas autónomas ¿quiénes serán responsables de cualquier violación del derecho internacional? Ya que no se pueden ser transferidas a una máquina, programa de computadora o sistema de armas.

3. ¿Qué límites son necesarios para la autonomía de los sistemas de armas garanticen el cumplimiento del DIH?

4. ¿Las armas autónomas aumentarían o disminuirían el control humano en la guerra tomando en cuenta que la esencia de las armas autónomas es que los humanos han delegado la toma de decisiones de fuerza letal en la máquina?

5. ¿Un sistema autónomo podría ser el soldado perfecto, haciéndolo más predecibles que los humanos en una crisis y evitando violaciones al DIH?

6. ¿El juicio humano es indispensable para la gestión de crisis?

7. ¿Cuáles serían las exigencias mínimas de seguridad para garantizar que los sistemas de armas autónomas no sean intervenidos por agentes externos?

8. ¿En qué circunstancias las armas autónomas pueden representar una amenaza a la paz y seguridad internacionales?

9. ¿Es necesaria una regulación a este tipo de armas para evitar la amenaza a la paz y seguridad internacionales?

10. ¿Existe un concepto universalmente aceptado que permita una regulación eficiente?

11. ¿En caso de regulación cuales serían los mecanismos de auditoría?

INTELIGENCIA ARTIFICIAL (IA)

Antes de continuar es importante señalar qué se entiende por inteligencia artificial o IA, aquella que abarca los métodos para la percepción automatizada, el aprendizaje, la comprensión y el razonamiento informatizados, que se han convertido en algo común en nuestras vidas, valiéndose para ello de ciencias auxiliares tales como la lógica, las matemáticas, la informática y la filosofía.

Continuando con lo expuesto anteriormente el crecimiento de la eficacia y la ubicuidad de los métodos de IA también han estimulado a pensar en los riesgos potenciales asociados con la misma. Es natural que el avance de las tecnologías pueda desencadenar nuevas y emocionantes capacidades y aplicaciones así como también generar ansiedades nuevas.

Por estas mismas razones ya alrededor de 26 especialistas en IA, ciberseguridad y robótica de prestigiosas universidades como Cambridge, Oxford, Yale, Stanford, así como de organismos no gubernamentales (OpenAI, Center for a New American Security, Electronic Frontier Foundation), alertan en su informe “The Malicious Use of Artificial Intelligence” que en la próxima década la eficacia creciente de la inteligencia artificial (IA) podría potenciar la cibercriminalidad amenazando la seguridad de los países, sus dirigentes e incluso procesos electorales.

Una preocupación latente son los ciber-ataques, continuamente nuestros ordenadores son atacados con virus y otras formas de malware y los algoritmos de IA no son diferentes a los de otros programas por lo cual pueden ser vulnerados. La preocupación viene de la mano según el nivel de complejidad y dependencia de las funciones en las que se usa IA. Sin embargo en todas partes del mundo se fomentan y financian una amplia gama de proyectos de investigación de seguridad cibernética, orientados a dar a la IA las herramientas necesarias para que sea capaz de detectar y suprimir los ataques cibernéticos.

También es importante resaltar que el sector de la ciberseguridad es uno de los que, en mayor medida, están siendo afectados por la IA. En el aspecto positivo, está contrastada su capacidad para reducir las ciberamenazas, mejorando la detección de ataques. Pero en la carrera por su utilización también están involucrados grupos de crimen organizado y hackers, que recurren

crecientemente a la IA para perfilar los ataques, seleccionar un mayor número de objetivos de forma más dirigida y menos indiscriminada, mejorando su eficiencia pudiendo ser replicados en numerosos equipos. Adicionalmente, la IA podría ser una vía para hackear dispositivos conectados a internet, vehículos o drones, tomando el control de los mismos con intenciones delictivas o criminales. Todos estos crímenes pueden ser perpetrados sin ser detectados y mucho menos atribuirse responsables.

Así mismo la IA podría facilitar la manipulación de elecciones políticas, amenaza que puede plantear serios problemas a la estabilidad política de algunos países y tal vez desencadenar graves conflictos, ya sean nacionales o internacionales. Estas preocupaciones son más significativas en el contexto de Estados autoritarios. Así pues la IA ofrece oportunidades colosales, pero también amenazas difíciles de predecir, aumentado el riesgo de que algunos Estados la utilicen para el control social de los ciudadanos o para reforzar su competencia geopolítica a nivel internacional

En toda la historia humana, la política ha sido impulsada fundamentalmente por la acción humana consciente y las acciones e interacciones colectivas de los seres humanos dentro de las redes y organizaciones. Ahora, los avances en inteligencia artificial (IA) mantienen la perspectiva de un cambio fundamental ya que la idea de una entidad no humana con una agenda específica podría crear un cambio radical en nuestra comprensión de la política en los niveles más amplios. En funciones analíticas, los sistemas de inteligencia artificial pueden permitir que menos humanos tomen decisiones de mayor nivel, o automatizar tareas repetitivas tales como monitorizar los sensores establecidos para garantizar el cumplimiento de un determinado tratado.

En estos roles, la IA bien puede cambiar, y de alguna manera ya ha cambiado, las estructuras a través de las cuales los encargados de tomar decisiones entienden el mundo, a largo plazo, tales sistemas podrían transformar radicalmente no solo la forma en que se toman las decisiones, sino también la forma en que se llevan a cabo. Es así que la IA marca uno de los avances más disruptivos de los próximos años, configurando el poder geoestratégico del futuro, al igual que la evolución social. En consecuencia, Los países más desarrollados han iniciado una carrera con el objetivo de liderar las capacidades generadas por el uso de la IA, que se presenta como un indicador del presente y futuro liderazgo internacional, principalmente en tres dimensiones de poder: la económica, la militar y la informativa.

En la dimensión militar se está produciendo una carrera entre los principales productores de la industria armamentística del mundo para optar al liderazgo geoestratégico, geopolítico y geoeconómico. La irrupción de la IA altera las

capacidades ofensivas y defensivas, como ya sucedió con la tecnología aeroespacial, la nuclear, la cibernética y la biotécnica.

“La IA posibilitará introducir autonomía o semi-autonomía en robots, acelerará el uso de aviones de combate no tripulados, desarrollará artefactos explosivos improvisados móviles y robóticos y se incorporará a sistemas armamentísticos” (lethal autonomous weapon systems). Representando así desafíos en el campo militar (nucleares, Aero espaciales, cibernéticos y biotecnología).

Es importante ahondar en las implicaciones sociales, políticas, económicas y existenciales que provocarán estos escenarios y definir mecanismos de control que garanticen la seguridad futura, para ello hay que garantizar una mayor supervisión y transparencia de los gobiernos en esta materia con el objetivo de dar recomendaciones para el adecuado uso de la financiación y prioridades de investigación para evitar su desarrollo inadecuado haciendo énfasis en el apoyo a la implementación pacífica de la IA, también se necesitan códigos de conducta claros para garantizar que los beneficios de la IA se puedan compartir ampliamente, mientras que sus riesgos concurrentes están bien gestionados. Todo esto si queremos darle un futuro más cierto y más humano a las próximas generaciones ya que la IA confiere considerables ventajas en materia de defensa y ataque militar frente a las estrategias y el armamento convencional.

En 1979 se creó en USA la AAAI (Asoc. para el Avance de la IA) cuya misión es doble: avanzar en la ciencia y la tecnología de la inteligencia artificial y promocionar su uso responsable. La AAAI considera que los riesgos potenciales de la tecnología de la IA deben constituir un escenario importante para la reflexión, la prevención y el avance. Si se prevén los riesgos, se pueden evitar. Ejemplos como este son necesarios y podrían ser de utilidad en experiencia recorrida para lograr una mejora en la implementación de la IA, Las recomendaciones pasan por reforzar las capacidades de la ciberseguridad, incorporar nuevas normas para prevenir A posibles abusos de la misma y promover la cultura de la responsabilidad potenciando la educación y la ética,
Nuestros avances tecnológicos son beneficios, nadie lo puede negar, con ellos curamos enfermedades, solucionamos problemas que afectan la actividad cotidiana de la sociedad, pero también tiene el poder de destruir, como por ejemplo bombas atómicas y armas biológicas. Estos cambios sin duda traerán a la humanidad avances positivos en la resolución de problemas globales, pero no se debe dejar de lado los riesgos que también generará, en seguridad interacional específicamente, por lo que los gobiernos deben tener como precedente los anteriores avances para evitar cometer los mismos errores y utilizarla de forma ética tomando en cuenta la capacidad de adaptación y resiliencia en la historia de la humanidad.

PREGUNTAS CLAVES

- ¿Es necesario trabajar sobre la gobernanza nacional e internacional de la IA?
- ¿Será necesario reforzar las capacidades de la ciber seguridad?
- ¿Es oportuna la creación de una agencia Internacional de inteligencia artificial dependiente de la ONU?
- ¿Cómo alertar ante nuevos riesgos?
- ¿La IA se plantea como aliada de los ciberataques o de la seguridad?
- ¿Cómo pueden aplicarse los avances en la gestión de las relaciones internacionales entre países?
- ¿Cuáles serán sus traslaciones en áreas como seguridad militar, humana y las perspectivas económicas?
- ¿Es una potencial amenaza a la seguridad?
- ¿Cómo la IA cambia la manera en que tenemos que pensar en los asuntos internacionales?

CIBERSEGURIDAD EN TIEMPOS DE CONFLAGRACIÓN.

Al estar la tecnología tan presente y siendo tan indispensable para la humanidad, no resulta extraño que esta sea el nuevo “campo de batalla” entre la lucha de intereses que múltiples grupos humanos puedan tener, tal razón amerita que en el plano de la Seguridad Internacional del Siglo XXI sea menester abordar la seguridad en el plano cibernético, al lograr la globalización, la ruptura de barreras físicas entre los seres humanos. Podemos entender a la ciberseguridad como aquellas medidas de protección ante usos delictivos del internet, actividades de espionaje por razones políticas o económicas, sabotajes a estructuras críticas como las comunicaciones, el transporte y la energía, propaganda y contra-información (fake news) que lleva a las naciones y a la comunidad internacional a abordar estrategias conjuntas en esta materia.

Y no es para menos, bajo el entramado cibernético (entiéndase, el ciberespacio y el universo de plataformas digitales que la tecnología ofrece) reposa información valiosa para cada individuo, sociedad y Estado, la cual, partiendo de la confiabilidad que se le confiere a la seguridad cibernética reposa en su haber importantes activos de “interés nacional/internacional” que van desde transacciones financieras, archivos de inteligencia y espionaje, documentación clasificada y hasta códigos de programación nuclear, y ha sido tanta la importancia de este apartado (seguridad cibernética, repetimos) que precisamente aquellos activos que esta se encarga de proteger, son los que

han definido en buena manera la política y la diplomacia internacional en el orden mundial Post-Segunda Guerra Mundial y Post-Guerra Fría.

De acuerdo a tal orden de ideas, las Naciones Unidas a través de sus múltiples organismos ha manifestado la importancia de la ciberseguridad, al calificar el cibercrimen como una evolución de la delincuencia trasnacional. La naturaleza compleja del crimen como una que tiene lugar en el ámbito sin fronteras del ciberespacio se ve agravada por la creciente participación de los grupos del crimen organizado. Los perpetradores del delito cibernético y sus víctimas pueden ubicarse en diferentes regiones, y sus efectos pueden repercutir en las sociedades de todo el mundo, destacando la necesidad de organizar una respuesta urgente, dinámica e internacional.

A pesar del impacto que siguen generando actividades de crimen organizado ya conocidas como el narcotráfico y el lavado de dinero, resulta preocupante el crecimiento de otro tipo de actividades criminales donde su naturaleza reside en las tecnologías de información y comunicación (TIC). En la actualidad, los usuarios de internet representan el 53% de la población mundial (4021 millones de personas) según los datos del reporte anual Global Digital elaborado por distintas firmas de estadísticas a nivel mundial. Debido a esto podemos medir el alcance de la susceptibilidad que posea alguna persona, empresa o institución en la actualidad de ser víctima de alguna distorsión en el uso del internet.
La información o data es la esencia de la interacción en entornos digitales, por ende, el resguardo y seguridad de toda la información circulante en internet ha sido uno de los principales retos de las empresas basadas en tecnología y de los sectores legales de preservar la integridad de los usuarios en estos entornos digitales. Por esta razón podemos definir al Cibercrimen como todas aquellas actividades ilícitas en internet basadas en dos escenarios: 1) El secuestro, robo, malversación, uso indebido o usurpación de la data privada de personas, empresas o instituciones; 2) La implementación de códigos maliciosos para la alteración en el funcionamiento de plataformas digitales (Hacking).
A continuación, definimos algunos de las técnicas de cibercrímenes más conocidos en la actualidad:

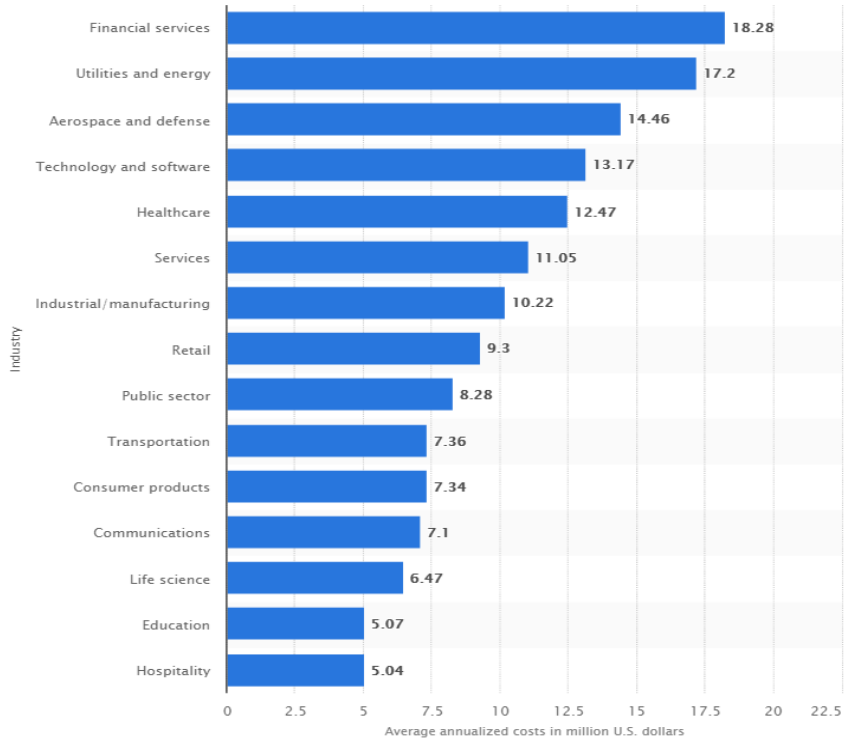
- **Malware:** El malware es un código o archivo enviado a través de la red con el fin de infectar, robar información o interrumpir el funcionamiento de los dispositivos. Según un informe de Kaspersky Lab (Empresa de seguridad informática), entre agosto de 2015 y agosto de 2016 hubo más de 398 millones de ataques con malware registrados en Latinoamérica, un promedio de 12 ataques por segundo.

- **Ransomware:** El ransomware asume el control de acceso del administrador e impide que los usuarios accedan a todos o algunos

sistemas. Los atacantes fuerzan a sus víctimas a pagar una recompensa por medio de diversos métodos de pago en línea, antes de desbloquear sus sistemas. Estas formas de malware infiltran los sistemas operativos por medio de mensajes de email o de descargas falsas. Uno de los ataques con Ransomware más conocido fue el del pasado año 2017 que afectó alrededor de 300.000 organizaciones en todo el mundo, entre ellas el Servicio Nacional de Salud (NHS) del Reino Unido, la empresa Telefónica en Madrid y el Ministerio Interior Ruso.

- **Phishing:** consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

En la siguiente grafica podemos observar los costos anuales promedios expresados en millones de dólares relacionados a incidentes de delitos cibernéticos a partir de agosto del 2017, además de observar cuales son los sectores más afectados por estas actividades.



Costos y sectores más afectados por delitos informáticos
Statista - 2018.

Con todo esto en mente podemos observar la importancia que tiene la seguridad informática para las empresas e instituciones en la actualidad. Por esta razón, países como Estados Unidos han generado apartados especiales en sus inversiones para potenciar y mejorar la rama de ciber-seguridad en sus actividades.

La Oficina de las Naciones Unidas contra la Droga y el Delito promueve la creación de capacidad a largo plazo y sostenible en la lucha contra el delito cibernético mediante el apoyo a las estructuras y acciones nacionales. Específicamente, la ONUDD recurre a su experiencia especializada en respuesta a los sistemas de justicia penal para proporcionar asistencia técnica en creación de capacidad, prevención y sensibilización, cooperación internacional y recopilación de datos, investigación y análisis sobre ciberdelincuencia.

Sin embargo, la preponderancia que las Naciones Unidas le dan a la prevención de los delitos cibernéticos como manifestación de la delincuencia trasnacional, también tiene en contraposición la importancia de preservar (entre muchos otros) el derecho humano a la privacidad, tal como hizo saber en mayo de 2018 el relator especial sobre el derecho a la privacidad Joseph Cannataci ante el CDH-ONU –UNHCR– destacando el equilibrio que debe residir entre la privacidad y la seguridad en el ciberespacio, a lo cual hemos de sumar, el pulso entre naciones a nivel geopolítico hace que los conflictos de **Cuarta Generación** escalen a un nuevo nivel donde si bien la guerra avanza al paso del desarrollo tecnológico y las relaciones internacionales, no es menos cierto que del mismo modo deben avanzar los derechos humanos, las libertades individuales y el acceso a la información de conformidad a las **OBJETIVOS Y METAS DE DESARROLLO SOSTENIBLE (AGENDA 2030)**, todo en una suma de factores que implica mantener (por sobre todo, como fin principal del CS-ONU –UNSC–) la paz y seguridad internacional, dejando en claro una vez más, que el interés de cada Estado-Nación frente a la seguridad cibernética es un punto de debate bastante álgido en lo que respecta a mantener la delgada línea entre seguridad y libertades.

CONCLUSIONES Y RECOMENDACIONES

En base a lo anteriormente expuesto en cada uno de los temas abordados, podemos observar la estrecha relación existente entre ellos, por un lado la Inteligencia Artificial en la robótica brinda grandes beneficios a la humanidad, pero a su vez, es utilizada en la industria militar para la configuración de las armas autónomas y a su vez para la generación de malware que vulneran los sistemas informáticos. En este sentido, el Consejo de Seguridad entra en discusión de estos tópicos bajo la premisa que estos instrumentos al permitirse su desarrollo indiscriminado puede, como seguramente lo hará, transgredir los

principios del derecho internacional, la capacidad de maniobra de los Estados y por ende de la seguridad internacional.

En este sentido es menester que el Consejo de Seguridad se aboque en delimitar la usabilidad y desarrollo de estas herramientas desde el punto de vista técnico y normativo, asimismo diseñar estrategias de seguridad para contrarrestar posibles ataques y prevenir los mismos de la mano con un sistema de monitoreo y contra oportuno.

El cibercrimen cada vez es más común dentro del panorama actual, y a pesar de los planes de acción existente de forma unilateral los métodos de respuesta inmediata multilateralmente no están a la altura de circunstancias que pueden potenciar estos ataques; en este orden de ideas, estas tres variables facilitan el ciberespionaje, inclusive entre Estados, lo cual es un conducta completamente contradictoria a los preceptos de soberanía y libre determinación, conducta frente a la cual este organismo debe trazar una ruta.

Finalmente, recordando que este comité será abordado bajo la modalidad de agenda abierta, el enfoque temático esta entendido como todos aquellos elementos del desarrollo tecnológico de última generación propios de la cuarta revolución industrial que en la actualidad carecen de marcos regulatorios y constituyen una vulneración a la seguridad de los Estados y la comunidad internacional; de tal manera que se esbozan en esta guía de estudio tres ejemplos de estos casos (Inteligencia Artificial y robótica, Armas Autónomas, y Ciberseguridad) queda a merced de los dignos representantes de Estados Miembros de este Consejo definir en la primera sesión de debate cual o cuales temas serán tratados, pudiendo abordar inclusive enfoques que no hayan sido mencionados en esta guía siempre guarden estrecha correlación con el enfoque temático.

Enfatizando que la discusión de un tema no deberá exceder las 4 sesiones de debate, y la agenda a seguir durante los tres días de jornada tendrá obligatoriamente que ser definida en la primera sesión de debate, de lo contrario, la mesa directiva lo decidirá por oficio en base a los argumentos esgrimos por los diferentes representantes.

REFERENCIAS

- Comité Internacional de la Cruz Roja (CICR), “A guide to the legal review of new weapons, means and methods of warfare measures to implement article 36 of additional protocol I of 1977”, noviembre de 2006, [en línea] disponible
  en: https://www.icrc.org/eng/assets/files/other/icrc_002_0902.pdf,

- Human Rights Watch, “Losing Humanity: the case againts killer robots” (2012), [en línea] disponible en: http://www.hrw.org/reports/2012/11/19/losing-humanity-0,

- Altas Partes Contratantes de la CCW, “informe final del período de sesiones de 2013”, documento CCW/MSP/2013/10, Ginebra, 16 de diciembre de 2013, [en línea] disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/646/36/PDF/G1364636.pdf?OpenElement

- Tercera (3ª) reunión informal de expertos sobre sistemas de armas autónomas letales celebradas en el marco de la CCW, “draft recommendations”, Ginebra, 15 de abril de 2016, [en línea] disponible en: http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2016/meeting-experts-laws/documents/DraftRecommendations_15April_final.pdf,

- Dr. Jacob Parakilas, Mary L. 'Missy' Cummings, Dra. Heather Roff, Kenn Cukier y Hannah Bryce, *¨Inteligencia artificial y asuntos internacionales, interrupción prevista¨*, junio de 2018, [en línea] disponible en: https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf

- Rodrigues Bernardo “*Inteligencia Artificial Y Robotización: Una Odisea Humana*”, Abril de 2018, en línea] disponible en: http://www.seguridadinternacional.es/?q=en/node/1368

- Blanco Jose Maria y Cohen Jessica *¨Inteligencia artificial y poder¨*, julio de 2018, [en línea] disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari93-2018-blanco-cohen-inteligencia-artificial-poder

- Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, y otros, *´´The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation´´*, febrero de 2018, [en línea] disponible en: *https://maliciousaireport.com/*

- Allen Greg y Chan Taniel *¨Artificial Intelligence and National Security¨*, Julio de 2017, [en línea] disponible en: *https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf*

- Pascual Álvaro, ¨*Inteligencia Artificial: Un Panorama De Algunos De Sus Desafíos Éticos Y Jurídicos*¨ [en línea] disponible en: https://dugi-doc.udg.edu/bitstream/handle/10256/14950/alvaro-pascual.pdf?sequence=1

- Yanez Rayn ¨La Participación de la Inteligencia Artificial en la Seguridad Internacional

- [en línea] disponible en: http://www.academia.edu/32131610/La_Participaci%C3%B3n_de_la_Inteligencia_Artificial_en_la_Seguridad_Internacional