SC

SECURITY COUNCIL

CYBERNETIC WEAPONS

SECRETARIA GENERAL:
MÓNICA DANAÉ JUÁREZ LÓPEZ

PRESIDENTE:
SHAYLA KIMBERLY WEST

MODERADORES:
JESÚS LEONARDO CABRERA MEJÍA
FRANCISCO RODRÍGUEZ GARCÍA MUÑOZ

TECMI MUN 2019

CARTA DE BIENVENIDA

Queridos delegados, organizadores y faculties asistentes a TECMIMUN 2019 – Campus Villahermosa.

Es todo un honor para mí dirigirme a ustedes como la primera Secretaria General del Modelo de las Naciones Unidas de la Universidad Tecmilenio. Me siento entusiasmada de ser parte del Comité Organizador de la Primera Edición de TECMIMUN, el cuál se llevará acabo los días 24 y 25 de mayo, 2019.

Todo comenzó como iniciativa de cinco alumnos con el sueño de formar parte de la red de Modelos de Naciones Unidas en el estado de Tabasco y ser parte del desarrollo de habilidades de los jóvenes de hoy. Buscamos el apoyo de nuestro Campus y de tal manera, formar el comité organizador. Dicho comité se caracteriza por el entusiasmo, creatividad, compromiso, responsabilidad, el ser proactivos y sobre todo la pasión que cada uno de nosotros tiene por este proyecto que hoy es una realidad.

Con este modelo desarrollarás diversas habilidades entre las cuales destaca el poder solucionar problemáticas que observamos día a día, administración del tiempo y planeación, dominio de la situación, mejorar nuestras relaciones al interactuar con jóvenes con quienes no convivimos regularmente y conocer cada vez más acerca de lo que sucede a nuestro alrededor y como estas acciones repercuten en nosotros.

Para finalizar, me gustaría reiterar la alegría que me genera el que ustedes formen parte de esta historia que apenas comienza, y recuerden; "Sólo existen dos días en el año en que no se puede hacer nada. Uno se llama ayer y otro mañana. Por lo tanto, hoy es el día ideal para amar, crecer, hacer y principalmente vivir". (Dalai Lama) Por lo tanto, hoy es el día ideal para formar parte de TECMIMUN 2019.

Atentamente:
Mónica Danaé Juárez López
Secretaria General
TECMIMUN 2019

Universidad Tecmilenio

TECMI MUN 2019

AGENDA
VIERNES 24 DE MAYO

MAÑANA

07:50 - 08:50	REGISTRO
09:00 - 10:00	APERTURA
10:30 - 11:50	PRIMERA SESIÓN

TARDE

12:00 - 12:25	RECESO
12:30 - 13:55	SEGUNDA SESIÓN
14:00 - 16:00	COMIDA
16:10 - 17:55	TERCERA SESIÓN
18:00 -18:25	RECESO
18:30 - 20:00	CUARTA SESIÓN

NOCHE

SIN EVENTOS

AGENDA
SÁBADO 25 DE MAYO

Universidad Tecmilenio

TECMI MUN 2019

MAÑANA

08:00 - 09:25	QUINTA SESIÓN
09:30 - 09:55	RECESO
10:00 - 11:55	SEXTA SESIÓN

TARDE

12:00 - 12:25	RECESO
12:30 - 13:55	SÉPTIMA SESIÓN
14:00 - 16:00	COMIDA
16:10 - 17:55	OCTAVA SESIÓN
18:00 -18:25	RECESO
18:30 - 19:30	NOVENA SESIÓN

NOCHE

20:00 - 21:00	CLAUSURA

PROTOCOLO

En el modelo de las Naciones Unidas de la Universidad Tecmilenio Campus Villahermosa, TECMIMUN, existen mociones y puntos. Las mociones demandan un proceso de votación para ser aprobadas. En cambio, los puntos, se aplican de manera inmediata. Existen diferentes tipos de votos; entre ellos se encuentran, a favor, en contra y abstención.

Sin embargo, puede haber ciertas excepciones en las que abstenerse no está permitido. En estas situaciones el moderador le hará saber al comité.

MOCIONES

• Moción para establecer la agenda / Motion to establish the agenda: Establecer tiempo, número de preguntas y número de subsecuentes/follow ups.

• Moción para abrir la lista de oradores / Motion to open the speaker's list:
Los delegados que realizaron y secundaron la moción, ocuparan el primer y segundo lugar de la lista, respectivamente.

• Moción para reabrir la lista de oradores / Motion to reopen the speaker's list:
 Esta moción puede ser hecha una vez por sesión a partir de la segunda sesión. Si la moción pasa, tres movimientos pueden ser realizados, independientemente de que sean aprobados por el foro o no.

• Moción para añadir a (nombre del país) a la lista de oradores / Motion to add (country's name) to the speaker´s list:

Si la moción pasa, el país agregado ocupa el último lugar de la lista. El delegado no puede rehusarse a participar en la lista de oradores una vez añadido; de lo contrario, recibirá una amonestación escrita.

Moción para mover a (nombre del país) al primer lugar/segundo lugar/tercer lugar de la lista de oradores / Motion to move (the country's name) to the first place/second place/third place in the speaker's list:
Si la moción pasa, el país se mueve al primer lugar en la lista. Si un país ya ha sido movido allí, el país debe moverse al segundo o tercer lugar de la lista.

• Moción para abrir una sesión extraordinaria de preguntas / Motion to open an extraordinary sesión of questions:
El número de preguntas debe ser especificado. Esta moción puede ser hecha una vez que el número de preguntas de la agenda haya terminado. Mientras el delegado está hablando para realizar la moción, otros delegados pueden alzar su personificador para ser considerados en el número de preguntas para la moción. El moderador le preguntará al delegado que está al frente si acepta la sesión extraordinaria de preguntas. Si el delegado las acepta, el moderador procederá con la votación. Si no, la moción se cancela. Se puede hacer un máximo de dos sesiones extraordinarias de preguntas por delegado en cada sesión; si se necesitan más preguntas, se recomienda hacerlas durante un caucus moderado.

• Moción para abrir un caucus moderado / Motion to open a moderated caucus:
El tiempo y propósito deben ser establecidos, (discutir el tema: Es el primer propósito de un caucus moderado, mostrando la opción de poder debatir acerca de la cuestión más importante en ese momento/discutir soluciones:

Es la oportunidad en la cual los delegados pueden debatir acerca de las bases que estos tienen para poder encontrar una conclusión al problema). Se trata de un debate más fluido y directo entre delegados. Para hablar los delegados sólo deben levantar su personificador y esperar hasta que se les de la palabra. Los delegados que promovieron y secundaron serán los primeros en hablar durante el caucus.

Moción para abrir un caucus inmoderado / Motion to open a unmoderated caucus:

El tiempo y propósito deben ser establecidos. Éste es un debate en el que los delegados pueden levantarse de sus asientos y formar grupos o "bloques" para trabajar en los documentos requeridos por el comité, Papel de trabajo: Es un documento en donde se encuentran las bases de las primeras soluciones que las delegaciones dan al tema, ya que se dividieron en diferentes bloques, habrá discrepancia en las soluciones, aunque el propósito sea llegar a un documento en el que todos los delegados estén de acuerdo, esto, con un proceso de votación. Resolución: Es el documento final trabajado por todo el comité, en donde se usan frases operativas y pre ambulatorias, al final se hace un proceso de votación por el comité, y si este pasa, será llevado a otro comité para su votación final.

Nota: No todos los comités tendrán que pasar a otro foro.

• Moción para extender el tiempo del caucus moderado o inmoderado / Motion to extend the time of the moderated or unmoderated caucus:

El tiempo y propósito deben ser establecidos. Esta moción extiende el tiempo del caucus una vez que el tiempo inicial ha terminado. Extender el tiempo del caucus una segunda vez no está permitido, un nuevo caucus

debe de ser abierto en su lugar. Si el caucus es inmoderado, todos los delegados deben tomar asiento para poder realizar la moción.

Nota: Las extensiones no deben ser mayores al tiempo original.

• Moción para cerrar el caucus moderado o inmoderado / Motion to close the moderaded or unmoderated caucus:

Esta moción concluye el caucus si aún resta tiempo. Esta moción es recomendada sólo si no hay nada más que discutir por el momento.

Moción para introducir el papel de trabajo A/B o papel de resolución / Motion to introduce the working paper A/B or the resolution paper:

Si la moción pasa, dos delegados del bloque correspondiente deberán pasar al frente a dar lectura al documento y responder las preguntas del foro. Al no pasar la moción para leer alguno de los papeles de trabajo, inmediatamente pasa el otro bloque (si ninguno de los dos bloques pasa a leer, serán acreedores a una amonestación escrita).

• Moción para comenzar el proceso de votación para el papel de resolución / Motion to start the voting process of the resolution paper:

Si la moción pasa, la lista se pasará tres veces para votar por el papel de resolución. En la primera ronda se podrá votar a favor, en contra o abstenerse. En la segunda ronda se podrá votar a favor, en contra o abstenerse y se podrá utilizar el derecho de explicación, con el que los delegados pueden dar su punto de vista para exponer el motivo de su voto al término de esa ronda. En la tercera ronda solo se permitirá votar a favor o en contra de la resolución. En caso que la mayoría de los votos sean en contra, los delegados deberán hacer modificaciones a este documento.

• Moción para posponer la sesión / Motion to postpone the session: Esta moción es necesaria para terminar la sesión. En la mayoría de los casos, el moderador le hará saber al foro cuando estaría en orden hacer esta moción.

• Moción para cerrar el debate / Motion to close the debate: Esta moción indica el cierre del debate.

PUNTOS

• Punto de información / Point of information:
Este punto se usa para hacer una pregunta al delegado que ha leído su posición oficial. Ya sea para las preguntas de la agenda, o de una sesión extraordinaria de preguntas. Este punto no debe de usarse en un caucus moderado.

• Punto de duda parlamentaria / Point of parliamentary inquiry: Este punto se usa para pedir información acerca del protocolo, preguntar si una moción está en orden, el tiempo del caucus actual, el número de preguntas de una sesión extraordinaria o el proceso del comité (siguiente acción dentro del foro).

• Punto de duda / Point of inquiry:
Este punto se usa para aclarar dudas propias del idioma del comité, si el delegado olvida o no sabe alguna palabra.

• Permiso para establecer un comentario / Permission to establish a comment:
Los delegados puedan hacer uso de este cuando el tiempo restante en la agenda sea cedido a comentarios.

- Permiso para un breve preámbulo / Permission for a brief preamble: Si un preámbulo es necesario para hacer una pregunta, el permiso debe pedirse justo después del punto de información.

PUNTOS DE APELACIÓN

- Punto de orden / Point of order:

Si el protocolo no se está ejecutando como debería. El delegado puede alzar su personificador en cualquier momento, siempre y cuando el punto de orden esté relacionado con los delegados que estén participando en ese momento en el debate.

- Derecho de réplica / Right of reply:

Si se le ha faltado el respeto al honor nacional. El delegado puede exigir una disculpa por parte del delegado que faltó al respeto.

- Punto de privilegio personal / Point of personal priviledge: Relativo al bienestar del delegado. Para necesidades personales como dejar el foro o quitarse el saco, un mensaje debe de ser mandado a la mesa. Este punto también puede ser usado si un delegado es inaudible o incomprensible al leer la posición oficial, contestando o haciendo una pregunta.

FRASES PRE AMBULATORIAS Y OPERATIVAS

FRASES PRE AMBULATORIAS	
Advirtiendo además	Advirtiendo con aprobación
Advirtiendo con pesar	Advirtiendo con preocupación
Advirtiendo con satisfacción	Afirmando
Alarmados por	Aprobando
Buscando	Conscientes de
Considerando	Convencidos
Creyendo plenamente	Dando la bienvenida
Dándonos cuenta	Declarando
Deseando	Enfatizando
Esperando	Expresando su aprecio
Expresando su satisfacción	Habiendo adoptado
Haciendo un llamado	Habiendo considerado
Habiendo estudiado	Habiendo examinado
Habiendo oído	Habiendo recibido
Lamentando	Observando
Observando con aprecio	Plenamente conscientes de
Profundamente arrepentidos de	Profundamente convencidos de
Profundamente molestos	Profundamente preocupados
Reafirmando	Reconociendo
Recordando	Refiriéndose
Teniendo en mente	Teniendo en cuenta

FRASES OPERATIVAS	
Acepta	Además invita
Además proclama	Además recomienda
Además recuerda	Además resuelve
Afirma	Alienta
Apoya	Aprueba
Comprueba	Condena
Confía	Confirma
Considera	Decide
Declara	Designa
Exhorta	Expresa su aprecio
Expresa su deseo	Expresa su satisfacción
Felicita	Finalmente condena
Ha resuelto	Ha llamado a
Incita	Lamenta
Llama la atención	Nota
Proclama	Recomienda
Recuerda	Respalda
Resuelve	Toma en Cuenta

PRE-AMBULATORY AND OPERATIVE PHRASES

PRE-AMBULATORY PHRASES	
Warning in addition	Warining with approval
Warning with regret	Warning with concern
Warning with satisfaction	Affirming
Alarmed by	Approving
Searching	Aware of
Considering	Convinced
Believing fully	Welcoming
Realizing	Declaring
Wishing	Emphasizing
Waiting	Expressing appreciation
Expressing satisfaction	Having adopted
Further recalling	Having considered
Having studied	Having examined
Having heard	Having received
Regretting	Observing
Observing with appreciation	Fully aware of
Deeply sorry for	Deeply convinced of
Deeply annoyed	Deeply worried
Reaffirming	Recognizing
Remembering	Referring
Keeping in mind	Taking into account

OPERATIVE PHRASES	
Accepts	Also invites
Also proclaim	Also recommends
Also remember	Also solves
States	Encourages
Supports	Approves
Proves	Condemns
Trusts	Confirms
Considers	Decides
Declares	Designates
Exhorts	Express apreciation
Express wish	Express satisfaction
Congratulates	Finally condemns
Has resolved	Have called to
Inicites	Regrets
Calling attention	Realizes
Proclaims	Reommends
Remember s	Supports
Solves	Taking into account

La decisión de la mesa es inapelable y debe ser respetada en todo momento. No existe una moción para quitar las amonestaciones de un delegado en TECMIMUN.

CÓDIGO DE VESTIMENTA

Debido a la relevancia y formalidad del evento, todos los participantes deberán vestir ropa tipo formal ejecutivo. De no cumplir con el código de vestimenta, los alumnos recibirán una <u>amonestación escrita</u> y de reincidir en esto, no les será permitido el <u>acceso al modelo</u>.

Los colores de la vestimenta de los delegados <u>no deben</u> ser llamativos o muy coloridos (Colores fosforescentes), deben ser apropiados a la formalidad del modelo.

Mujeres:
• Traje sastre.
• Vestidos o faldas con un largo de no más de 3 dedos o 5 cm arriba de la rodilla.
• Escotes no pronunciados.
• No se permiten, sandalias de piso, pantalones de mezclilla de ningún color, ni tenis.
• No se admiten gorras, lentes de sol ni sombreros durante los debates.

<u>Nota:</u> En caso de vestir blusas o vestidos sin mangas o tirantes, el uso de saco es obligatorio dentro de los comités.

Hombres:
• Traje sastre (camisa de manga larga, pantalón de vestir, saco, corbata o moño, cinturón y zapatos formales).

O bien:

- Camisa, pantalón de vestir, cinturón, zapatos formales. (Sin corbata o moño).
- No se admiten gorras, lentes de sol ni sombreros durante los debates.
- En caso de usar tirantes, el uso del cinturón no es necesario.

Nota: En todo momento se deben usar calcetines que cubran el tobillo; es decir, está prohibido el uso de tines.

AMONESTACIONES

Las amonestaciones son un aviso para evitar faltas al protocolo.

Existen dos tipos de amonestaciones, verbales y escritas.

Después de recibir tres advertencias se le otorga al delegado una amonestación verbal.

Después de recibir tres amonestaciones verbales se le otorga al delegado una amonestación escrita.

Al contar con dos amonestaciones escritas el delegado será retirado del comité por esa sesión.

Al acumular tres amonestaciones escritas, el delegado será expulsado del modelo.

Al contar con una amonestación escrita los delegados no podrán ganar premio como Mejor Delegado. Únicamente si su participación ha sido excepcional y ha contribuido al buen funcionamiento del debate, podrán ser candidatos a premiación de Excelente y Sobresaliente delegado.

Los participantes pueden ser acreedores a una amonestación VERBAL cuando:

• Se hable en primera persona (ejemplos: quiero, pienso, nuestro, podamos, hagamos, entre otros.)

• Se usen pronombres personales (yo, tú, él, nosotros, ustedes, entre otros.)

• Se mantenga contacto directo con otro delegado (comunicarse de forma directa con un participante dentro del comité).

- Se usen palabras no permitidas dentro del comité. (guerra, pobre, rico, potencia, blanco, negro, además de aquellas palabras establecidas como ofensivas por la mesa).
- Se introduzcan alimentos o bebidas a las sesiones, a excepción de las permitidas por la mesa.
- Se llegue a mandar mensajes con propósitos fuera del establecido

Nota: Cuando el delegado se hace acreedor a dos amonestaciones verbales por la misma causa y reincide una tercera vez, se le otorga una amonestación escrita.

Los participantes pueden ser acreedores a una amonestación ESCRITA cuando:
- Se llegue tarde o no se asista a una sesión.
- No respeten las decisiones de la mesa.
- Se incumpla con el código de vestimenta.
- **No cuente con su posición oficial impresa**, (una para la mesa y otra para la lista de oradores), misma que será solicitada por la mesa en la primera sesión.
- Algún dispositivo electrónico suene o sea usado indebidamente durante la sesión para fines que no sean buscar información o elaborar documentos del comité (Videojuegos, redes sociales, música, entre otros).
- El delegado proporcione información falsa o incorrecta (la información deberá estar justificada para su aplicación)
- Se use el teléfono celular para otro propósito que no sea usarlo como red móvil.
- Mantenga contacto con algún observador o faculty durante la sesión.
- Se hable en otro idioma que no sea el idioma oficial del comité.

- Se brinde un derecho de réplica de manera irrespetuosa o burlona.
- Se brinde un punto de orden de manera irrespetuosa o burlona.
- Se abandone el foro si previa autorización
- Se tenga algún trato irrespetuoso durante el modelo a algún participante, secretariado o directivos de alguna institución.
- Hacer uso de algún punto o moción de manera irrespetuosa o burlona.

ACCIONES QUE CAUSARAN LA EXPULSIÓN DEL MODELO:
- Se incumpla con el reglamento de la Universidad Tecmilenio.
- Se insulte o intimide a algún participante, miembro de la mesa, secretariado o directivo de alguna institución.
- Se hurte alguna propiedad.
- Se llegue a agredir física o emocionalmente a algún individuo que se encuentre dentro de la institución.
- Se dañe con intención algún utensilio de la Universidad, (llegado a perpetuar esta acción, el responsable, deberá ser conciliado con el pago del valor de la reparación o costo total si es irreparable).
- Uso de sustancias psicoactivas (alcohol, drogas o cigarrillos) durante los días del evento.
- Se llegue a perpetuar contra la propiedad intelectual, el uso del plagio, ya sea en papel de trabajo, posición oficial o resolución.

El protocolo de TECMIMUN no cuenta con una moción para retirar las amonestaciones de los delegados. No se permitirá el uso de una moción de este tipo.

Las decisiones tomadas por la mesa son incuestionables y deben ser siempre respetadas.

COMMITTEE'S HISTORY

The Security Council held its first session in January 17th, 1946 at Church House, Westminster, London. Ever since its first meeting, the Security Council has taken permanent residence at the United Nations Headquarters in New York City. It has also travelled to many cities, holding sessions in Addis Ababa, Ethiopia; Panama City, Panama; and in Geneva, Switzerland.

During the Cold War, continual disagreement between the United States and the Soviet Union made the Security Council an ineffective institution. In June 1950, when the Soviets were boycotted the Security Council over the issue of China's UN membership. Troops from South Korea, the United States, and 15 other countries would swell the ranks of United Nations Command to nearly 1 million by war's end. When the armistice that ended the Korean war was signed at P'anmunjŏm in July 1953, more than 250,000 troops—the overwhelming majority of whom were Korean—had died while fighting under the banner of United Nations Command in Korea.

Between the late 1980s and the early 21st century, the council's power and prestige grew. In the late 1980s, there was a surge in the number of peacekeeping operations (including observer operations) authorized by the security council. From 1948 to 1978 there had been authorized only 13 missions; this was a clear contrast to some 3 dozens operations that were approved between 1987 to 2000, including those in Balkans, Angola, Haiti, Liberia, Sierra Leone, and Somalia.

COMMITTEE'S MISSION

The Security Council takes the lead in determining the existence of a threat to the peace or act of aggression. It calls the parties in a dispute to settle it by peaceful means and recommends methods of adjustment or terms for the settlement. In some cases, in order to maintain or restore international peace and security, the Security Council can impose sanctions or even authorize the use of force.

SECURITY COUNCIL- NON-PROLIFERATION OF CYBERNETIC WEAPONS

Cybernetic weapons are defined as any piece of software used by an individual or organization in order to cause damage or steal information from another. These kinds of weapons are characterized for their use of networks and modern communication to spread and attack. Cyber-attacks usually consist of net-blocking, information stealth, corruption of information systems and classified document filtration.

The first registered attack took place in 2010 by a worm now known as Stuxnet. Stuxnet targeted an Irani computer system in charge of a Nuclear plant in order to smash its computer system. Since then, a variety of attacks have been executed to other delegations, organizations and companies.

The attacks can vary in severity. Considering the damaged caused to their targets, these are some of the most serious cyber-attacks to the day:

- The theft of personal information from more than 100 million credit cards from South Korea back in January 2014.
- The hacking of personal and banking information of 500 million users of the "Marriott" hotel chain.

- The stealing of 1.2 billion passwords from approximately 420 thousand sites in Russia during August 2014.
- The hacking of 3 billion users from "Yahoo!" in 2 different attacks during 2013.

Every day weapons and defensive systems are being developed in different zones and for different purposes. This phenomenon has led to a global, cyber warfare that involves any country with connection to networks and internet. This cyber warfare has given reasons to most countries to develop distinct types of software, spyware, malware, as well as intricate defensive/protection systems in order to protect from a possible attack or the start of a cyber-based conflict.

Certain hacker groups and weapons represent a threat, mainly because most of them aren't directly related to any government agency; and therefore, they aren't regulated and most of the time aren't subjected under federal laws. . and while these illegal groups are considered a big scale problematic, it's clear that the most powerful arsenal is in possession of distinct governments and security organs, from these weapons there are a few that outstand for its destructive potential and / or being involved in various attacks, such as:

- The collection of malware known as "Duqu"
- Middle Eastern originated malware known as "Flamer" or "Skywiper"
- Chinese attack tool "the great cannon"
- Japanese malware "未来" (meaning "future", being pronounced as "miray")
- Malicious computer worm "StuxNet"

- "Flamer" derived malware "Wiper"

The previously mentioned weapons and attacks are part of a growing weapon market used and developed mostly by illegal organizations and groups that have no regulations established by the United Nations; and, as a result, they cannot be arrested or stopped legally.

Cyber-attacks pose potential risk such as loss of capital, information, and security threats. In addition, cyber-attacks can cause long term problems like the corruption of systems in large companies, hospitals, or power plants (of different type of sources). These attacks can also target cryptocurrencies like Bitcoins and in doing so damage the economy of countries and organizations that use them. A side effect of an attack can be the loss of trust that clients might have when a company or website is targeted, reducing the numbers of clients and hence the income a company could get from them.

Some nations have already established their laws and solutions; yet these only work within the country and have no jurisdiction in foreign lands or organizations. In consequence to the limited jurisdiction of the countries, the only possible solution is making a treaty that regulates the actions taken after a cyber-attack. The treaty must explain clearly how and when countries should act after a cyber-attack and should include a definition of cybercriminal.

Throughout the debate it is fundamental to discuss these issues regarding cybernetic weapons:

- The limiting of internet connection as a measure taken by certain governments in order to control the possible attacks, and the privacy and freedom that would be taken from the user in the process.
- The high rates of governmental or personal information theft and selling done by big companies, governmental bodies and illegal hacking groups.
- The elevated prices of security related programs and organs that have to be developed by countries and companies in order to be prepared for a possible cyber attack.
- The lack of regulations related to the definition and penalties for cyber criminals and major cyber attacks.
- The economic imbalance that could be caused by an attack to cryptocurrency users around the world and any user of digital bank or non-physical currency.

COUNTRIE'S BACKGROUND

COUNTRY	FLAG	BACKGROUND
United States of America		Being the most cybernetically advanced country in security and weaponry matters, the United States has been part of various controversial events surrounding privacy and cybernetic attacks/weapons. it's also worth noting that this delegation has also been victim of attacks by hackers from other and the same nation in distinct moments.

French Republic		During 2015, France started a cyber security program in order to adapt to the new technologies that were entering the country and its society. This program was focused in the control of cyber-crime, protection of business, informing the public and maintaining the country's relevance in the international stage.
United Kingdom of Great Britain and Northern Ireland		Nothing a high worry for security, privacy and personal wellbeing of its citizens and companies, the UK has invested in cyber security and settled a number of offensive programs that haven't been used but are declared to be in response citing state actors, organized crime, terrorism, and individual criminals as major threats to the country in cyber-security matters.
People's Republic of China		There is an ongoing cyber warfare between the People's Republic of China and the United States of America that consists in accusations of which country is hacking which. An example of this was when the American company Mandiant accused China of espionage in 2013. China has taken a defensive position in relation to these accusations by denying any type of Chinese hacking, this has caused suspicions due to the existence of institutions backed by

		the government such as the People's Liberation Army and Information Engineering University whose purpose is to train future military hackers.
Russian Federation		The position of the Russian Federation consists in supporting the countries that are non-US allies in order to have a stronger front when cyber warfare actually happens. the Russian government has made very clear that they have the capacity of committing cyber attacks. Countries like the United States, the United Kingdom, and Australia have suspicions of cyber attacks already happening in their own country. Aside from the government related hackers, there are also Russian groups such as Fancy bear, Tsar team, Strontium, Sandworm, among others that are involved in the realization of cyber attacks and cyber crime.
Islamic Republic of Iran		Iran has been constantly involved in cyber conflicts with the United States, being responsible for major attacks and considered a growing threat. The first operations coming from the country were made by illegal hackers, but in various occasions the government has supported these groups and encouraged them to continue attacking the nations that are considered Iran's "Enemies".

State of Israel		Israel is considered one of the most involved countries in cyber security, it receives a big part (approximately 1/5) of the worlds private investment in security matters, and has a very important series of government-sponsored and independent hackers.
Republic of Korea		Being one of the most connected, and network advanced countries, the republic of Korea has been victim of various attacks due to its fast but insecure network and the previously mentioned dependence to connectivity. The government has already stablished cyber-security as a priority and reinforced the infrastructure in recent years after being victim to various major scale attacks to its privacy and governmental structure
Republic of Estonia		Estonia, being aware of the bigger picture of cyber- attacks not only in the main security and privacy of internet users but aware of the economic repercussions there can be, thanks to the concern of all these situations Estonia has considered cyber- security as an important point to address, not only in the Estonian territory but internationally, this has become an important topic not only in domestic affairs such as the theft of information and denial of

		services but it is important to look at it in a economic way that can affect everyone.
Kingdom of Netherlands		Cyber crime is an important issue in the Netherlands because of the uprising attacks there has been in the last couple years, this has affected the sustainability and safety of the internet community, and created a sense of being scared to what information is exposed, and how this affects not only social media but democratic elections and legal processes. Because of all the situations mentioned before the Netherlands is willing to make regulations in order to provide security to the community.
Kingdom of Denmark		Cyber security is a top priority in the Danish government, the problem is agreeing with most Danish political parties to get to a solution, a couple of opinions have come to an agreement to develop a six-year defense strategy. Another proposal is to use sensors to be aware of when a company or a government system is under malware attack in order to defend the information or what is in danger.
State of Japan		Japan has expressed its concerns in the Cyber Defense Unit, and how this might be upgraded in the future, not only to prevent as much cyber

		attacks as possible but to develop solutions that can make this task easier, this will affect the development of Japanese cyber defenses and will be a platform in order to upgrade the military aspect of this.
Democratic People's Republic of Korea		North Korea is considered to be a big threat in the cyber attack game, North Korean hackers are considered one of the most important ones nowadays, these compromise information and computer systems on a daily basis without being seen, an example of this is Pyongyang's, Lazarus Group one of the top system infiltrators.
State of Qatar		Qatar is a nation that doesn't count with any cybernetic weapons, but it has been involved in various conflicts, leading to this being an important topic for the country.
Ukraine		The country has been constantly under attack by the delegation of Russia, making Ukraine one of the most cybernetic attacked countries since these are constant. As a result, Ukraine has developed a strong defense line and made alliance with various countries to maintain the security of the country stable.
Kingdom of Norway		Even if the delegation hasn't been involved in any cybernetic conflicts, it counts with a defensive and offensive organ totally used for cybernetic conflicts, it's part of Norway's army

		and it's fully prepared for a cyber attack.
Republic of Ireland		It is a country fully prepared for an attack. This delegation has been preparing defenses since 2011; it has an organ dedicated to cybernetic security. In addition, the delegation has a big number of Irish companies and businesses employing cyber security services and preparing for a possible attack under any situation.
Saudi Arabia		Arabia has been a very important contributor to the expansion of cyber weapons. It has given a big amount of capital resources not only to defensive organs, but also various types of malware and spyware, weapons that had been used in external conflicts in the past.an example of this instances is the plot to attack the Iranian government during 2013, in collaboration with Israel.
Republic of India		This nation has been actively using malware to attack certain countries such as Pakistan. it's worth noting that alongside countries like Russia, North Korea and the United States, India figures as one of the most prepared countries in cybernetic matters being one of

		the nations that invest more capital resources to set up their systems.
Federative Republic of Brazil		Even if the major threat for Brazil is focused on organized crime, it's true that the country is now getting prepared with security updates, and heavily investing on cyber defensive programs for a possible warfare.it's also known that a big part of these security related programs have been acquired from the US government. And external organizations
Republic of Turkey		Turkey is highly at risk in case of a major cybernetic conflict. Even if the country counts with various organs destined to cyber security, it has been victim of quite a number of attacks during the last years, being clearly not in the level of other nations, Yet at the same time is one of the main internet and social media users/consumers.
Republic of Australia		Even though the country hasn't been involved in any cybernetic conflicts, it has been preparing defenses since 2008 and it declared that this kind of weapons represents a threat for the delegation and if necessary it will respond to the attacks.
Syrian Arab Republic		Cyber-related conflicts in Syria are mostly internal, due to the fact that the country is going through an armed conflict nowadays.

		The government has control of social media and other ways to expose the current situation in Syria. The use of cybernetic weapons in Syria is mostly related to the confrontation of citizens against Bashar Al-Assad and his reign. Having countries such as the Russian Federation and the Islamic Republic of Iran as allies in other matters also involves the contribution of resources in order to protect the Syrian government and its fragility.
Federal Republic of Germany		Berlin is one of the most targeted cities around the globe, causing concern in the future damage cyber attacks can do. The damages can affect power grids, drones, nuclear centrifuges, airport x-rays and medical equipment that could cause serious repercussion in the daily life of German people. In order to avoid the most part of this damage the German Government is developing a major program to protect its computer networks and supply systems. A new institution the National Cyber Defence Centre will be responsible for detecting potential threats, analyzing them and coordinating the necessary measures to disable the threat. In addition, a National Cyber Security Council will be established.

Kingdom of Thailand		Symantec is an American company that develops software and does annual reports about internet security. According to the report of 2018, the cybersecurity threat environment in Thailand ranked seventh-worst in Asia-Pacific, a dip from ninth in 2016. Also, it was found to be the 18th-worst worldwide when it comes to crypto mining attack threats, as well as the fourth-worst in Asia-Pacific. All of this means that in relation to countries in the same surrounding Thailand is found to be one of the most involved in cybersecurity situations as far as being one of the most affected due to the lack of security.
Republic of the Philippines		In past years the Philippines used to have a high ranking in the use of bitcoins so this alarmed the people who use this currency. The Philippines used to be a part of Operation Lotus Blossom which in collaboration with other countries such as Taiwan, Vietnam, Indonesia, Hong Kong, United States, and Canada had protection for any type of cyber issue, especially hacking.
Arab Republic of Egypt		Symantec a company that develops computer software released a name of a so called Leafminer whose purpose was targeting government organizations since 2017. There are many ways of intrusion to multiple

		websites some of these methods are: watering hole websites, vulnerability scans of network services on the internet, and brute-force/dictionary login attempts. All of this is related to the position of Egypt due to the fact that Leafminer was detected on aver 44 systems through the Middle East, and also in Egypt.
State of Libya		"Just before the American-led strikes against Libya in March 2011, the Obama administration intensely debated whether to open the mission with a new kind of warfare: a cyber offensive to disrupt and even disable the Qaddafi government's air-defense system, which threatened allied warplanes." This has been the only "recent news" about Libya being involved in any time of cyber warfare. Info from: https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html
Kingdom of Spain		Spain has been a victim of security breaches in telecommunication companies such as Telefonica. In 2017, Telefonica had a leak of personal information regarding the users of the company; while similar situations around the globe have occurred, the one in Spain is consider the biggest attack yet., Spanish

		companies have taken actions to reinforce their systems in order to avoid these type of events.
Republic of South Africa		The US Federal Bureau of Investigation has ranked South Africa sixth and seventh on the cybercrime predator list, this means that there has been struggles among the South African government because fraud is a raising issue in this country. As a response to this many corporations like Veromo Enterprises have hosted expositions in order to use these abilities to be part of an Industrial Revolution that helps youth.

BIBLIOGRAPHY

Commonwealth Parliament. (2013, November 7). Cyber security. Retrieved April 24, 2019, from https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber

Wikipedia contributors. (n.d.-a). Qatar. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Qatar

Wikipedia contributors. (n.d.-b). Qatar Armed Forces. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Qatar_Armed_Forces

Wikipedia contributors. (n.d.-c). Norwegian Cyber Defence Force. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Norwegian_Cyber_Defence_Force

Wikipedia contributors. (n.d.-d). Cyber Security Centre (Ireland). Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/National_Cyber_Security_Centre_(Ireland)

Wikipedia contributors. (n.d.-e). National Cybersecurity Authority (Saudi_Arabia). Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/National_Cybersecurity_Authority_(Saudi_Arabia)

Wikipedia contributors. (n.d.-f). Cyberweapon/ Probable cyberweapons. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Cyberweapon#Probable_cyberweapons

Wikipedia contributors. (n.d.-g). Flame (malware). Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Flame_(malware)

Wikipedia contributors. (n.d.-h). Great Cannon. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Great_Cannon

Wikipedia contributors. (n.d.-i). Wiper (malware). Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Wiper_(malware)

Wikipedia contributors. (n.d.-j). Stuxnet. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Stuxnet

Wikipedia contributors. (n.d.-k). Cyberweapon/Control and disarmament. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Cyberweapon#Control_and_disarmament

Wikipedia contributors. (n.d.-l). Cyberwarfare. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Cyberwarfare

Wikipedia contributors. (n.d.-m). Cyberwarfar in the United States. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Cyberwarfare_in_the_United_States

Wikipedia contributors. (n.d.-n). Kerala Cyber Warriors. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Kerala_Cyber_Warriors

Wikipedia contributors. (n.d.-o). Proactive cyber defence. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Proactive_cyber_defence

Wikipedia contributors. (n.d.-p). Cyber-arms industry. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Cyber-arms_industry

Wikipedia contributors. (n.d.-q). Cyberweapon. Retrieved April 23, 2019, from https://en.m.wikipedia.org/wiki/Cyberweapon

Turkey under cyber fire. (n.d.). Retrieved April 24, 2019, from http://turkishpolicy.com/article/850/turkey-under-cyber-fire

Cyber Security | Ministry of Foreign Affairs [Video file]. (n.d.). Retrieved April 24, 2019, from https://vm.ee/en/cyber-security

ABS-CBN News. (2015, June 17). How PH is defending against cyber attacks. Retrieved April 24, 2019, from https://www.youtube.com/watch?v=cSuPPYOUzwk&feature=youtu.be

ArtOfTheHak. (2018, July 25). Operation Lotus Blossom, 3 Minute Profile. Retrieved April 24, 2019, from https://www.youtube.com/watch?v=VMBAx4EdlEo&feature=youtu.be

Bangkok Post. (2018, July 20). Cybersecurity threats are on the rise in Thailand. Retrieved April 24, 2019, from https://www.scmp.com/news/asia/southeast-asia/article/2140073/cybersecurity-threats-are-rise-thailand

Brazil's Cybercrime Problem. (n.d.). Retrieved April 24, 2019, from https://igarape.org.br/en/brazils-cybercrime-problem/

Bryan Harris. (2018, June 6). South Korea warned of more cyber attacks ahead of summit. Retrieved April 24, 2019, from https://www.ft.com/content/783f20f0-692f-11e8-8cf3-0c230fa67aec

Chaim Levinson. (2018, December 9). Report: Israel Authorized NSO's Sale of Spyware to Saudi Arabia. Retrieved April 24, 2019, from https://www.haaretz.com/israel-news/report-israel-authorized-nso-s-sale-of-spyware-to-saudi-arabia-1.6725044

CNN. (2013, September 6). Cyber warfare: A way Syria could cripple the entire country [Video file]. Retrieved April 24, 2019, from https://www.youtube.com/watch?v=qJ9Ttn2K8Kw&feature=youtu.be

Cyber Security Strategy for Norway. (n.d.). Retrieved April 24, 2019, from https://sherloc.unodc.org/cld/lessons-learned/nor/cyber_security_strategy_for_norway.html

Cyber Weapons | Institute for Defence Studies and Analyses. (n.d.). Retrieved April 24, 2019, from https://idsa.in/taxonomy/term/1594

Defending Against Cyber Attacks in South Korea | KEI | Korea Economic Institute. (n.d.). Retrieved April 24, 2019, from http://keia.org/defending-against-cyber-attacks-south-korea

Dennis Miralis. (2018, September 28). What are Cyber Weapons? : Some Competing Definitions. Retrieved April 24, 2019, from https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906

export.gov. (n.d.). Retrieved April 24, 2019, from https://www.export.gov/article?id=Korea-Cyber-

Filippa von Stackelberg. (n.d.). Germany prepares for cyber war. Retrieved April 24, 2019, from http://www.newsecuritylearning.com/index.php/feature/88-germany-prepares-for-a-cyber-war

Gordon Corera. (n.d.). What made the world's first cyber-weapon so destructive? Retrieved April 24, 2019, from http://www.bbc.co.uk/guides/zq9jmnb

Irish businesses are âsitting ducksâ for cyber attacks. (2017, June 1). Retrieved April 24, 2019, from https://www.irishexaminer.com/business/irish-businesses-are-sitting-ducks-for-cyber-attacks-451353.html

Israel and Saudi Arabia are plotting a cyber weapon worse than Stuxnet – Cyber Defense Magazine. (n.d.). Retrieved April 24, 2019, from https://www.cyberdefensemagazine.com/israel-and-saudi-arabia-are-plotting-a-cyber-weapon-worse-than-stuxnet/

Laurens Cerulus. (2019, February 20). How Ukraine became a test bed for cyberweaponry. Retrieved April 24, 2019, from https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions. (n.d.). Retrieved April 24, 2019, from

https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Li Zhang. (n.d.). A Chinese perspective on cyber war. Retrieved April 23, 2019, from http://e-brief.icrc.org/wp-content/uploads/2016/09/43.-A-Chinese-perspective-on-cyber-war.pdf

Meet the 5 Russian Weapons of War Ukraine Should Fear. (2018, November 26). Retrieved April 24, 2019, from https://nationalinterest.org/blog/buzz/meet-5-russian-weapons-war-ukraine-should-fear-37112

Ministère de l'Europe et des Affaires étrangères. (n.d.). France and Cyber security. Retrieved April 24, 2019, from https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/

NCSC. (2015, December 1). Cyber Security Assessment Netherlands 2018 | NCSC. Retrieved April 24, 2019, from https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html

Newsweek. (2017, December 12). Iran's Cyber Warfare Program Is Now a Major Threat to the United States. Retrieved April 24, 2019, from https://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427

Oliver Joy. (n.d.). Mandiant: China is sponsoring cyber-espionage. Retrieved April 23, 2019, from

https://edition.cnn.com/2013/02/19/business/china-cyber-attack-mandiant/index.html

Patrick Tucker. (2018, November 26). Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says. Retrieved April 24, 2019, from https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/

Philippines ranked 5th in Bitcoin volume by currency | Jehzlau Concepts. (2017, November 3). Retrieved April 24, 2019, from https://www.jehzlau-concepts.com/2017/11/philippines-ranked-5th-in-bitcoin-volume-by-currency.html

Prashanth Parameswaran, The Diplomat. (n.d.). Japan-Philippines Defense Cooperation in Focus with Ministerial Meeting [Video file]. Retrieved April 24, 2019, from https://thediplomat.com/2019/04/japan-philippines-defense-cooperation-in-focus-with-ministerial-meeting/

S M Hali. (2017, July 29). Indian cyber weapon capability - Daily Times. Retrieved April 24, 2019, from https://dailytimes.com.pk/123434/indian-cyber-weapon-capability/
SABC Digital News. (2018, June 13). 2018 Cyber Security Indaba [Video file]. Retrieved April 24, 2019, from https://www.youtube.com/watch?v=fyDInVXL8No

Scott Ostergard. (2018, June 15). Russian "Sandworm" Hack Reveals 5-Year Cyber Espionage Campaign. Retrieved April 24, 2019, from https://www.ntconnections.net/blog/russian-sandworm-hack-reveals-5-year-cyber-espionage-campaign/

Security Zap. (n.d.). HomeCyber AttacksCyberspace and Cyber Warfare Capabilities of Iran Cyberspace and Cyber Warfare Capabilities of Iran. Retrieved April 24, 2019, from https://securityzap.com/cyberspace-of-iran/

Telefonica breach exposes personal data of 'millions' of customers | TheINQUIRER. (2018, July 17). Retrieved April 24, 2019, from https://www.theinquirer.net/inquirer/news/3035980/telefonica-breach-exposes-personal-data-of-millions-of-customers

The case for cyber weapons: India's strategy and goals. (n.d.). Retrieved April 24, 2019, from https://www.weforum.org/agenda/2017/10/the-case-for-cyber-weapons-india-s-strategy-and-goals/

The Economic Times. (2018, July 14). India is quietly preparing a cyber warfare unit to fight a new kind of enemy. Retrieved April 24, 2019, from https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-a-cyber-warfare-unit-to-fight-a-new-kind-of-enemy/articleshow/61141277.cms?from=mdr

Tom Jowitt. (2017, December 21). UK's Offensive Cyber Warfare Ability 'More Than Doubles' | Silicon UK Tech News. Retrieved April 24, 2019, from https://www.silicon.co.uk/e-regulation/governance/uks-cyber-warfare-ability-226365

Top China college in focus with ties to army's cyber-spying unit. (2013, March 24). Retrieved April 24, 2019, from https://www.reuters.com/article/net-us-china-cybersecurity-

university/top-china-college-in-focus-with-ties-to-armys-cyber-spying-unit-idUSBRE92N01120130324

United Nations Security Council |. (n.d.). Retrieved April 24, 2019, from https://www.un.org/securitycouncil/

VICE News. (2018, March 13). How Israel is becoming the world's top cyber superpower. Retrieved April 24, 2019, from https://news.vice.com/en_ca/article/evmyda/how-israel-is-becoming-the-worlds-top-cyber-superpower

WIRED Staff. (2018, December 8). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved April 24, 2019, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

TOP 10 of the world's largest cyberattacks | Outpost 24 blog. (n.d.). Retrieved April 25, 2019, from https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks