Cursos de Verano Complutense 2013

"CIBERSEGURIDAD, RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO"

"Los retos tecnológicos e industriales de la Ciberseguridad"

San Lorenzo de El Escorial, 3 de julio de 2013

General, señoras y señores, queridos amigos.

Es una gran satisfacción compartir este rato con ustedes, aquí en el marco incomparable que El Escorial proporciona. Quiero agradecer al Instituto Español de Estudios Estratégicos la oportunidad que me brinda de dirigirme a ustedes, dentro de esta nueva edición de los Cursos de Verano de la Universidad Complutense, para disertar sobre un tema que a una velocidad vertiginosa ha pasado de ser un asunto de unos pocos expertos, a tema de conversación corriente, habida cuenta de las noticias que proliferan en todos los medios de comunicación.

Quiero también resaltar que aunque voy a intentar ceñirme al tema específico que se me ha asignado, es prácticamente imposible no invadir temas o aspectos que ya hayan sido o vayan a ser tratados por el resto de los ponentes de este seminario.

Mi conferencia está estructurada en cuatro partes, relativamente diferenciadas. Empezaré con un breve bloque introductorio, seguido por un segundo en el que paso a enumerar los problemas y retos que una empresa como la nuestra tiene que afrontar desde la perspectiva de la ciberseguridad, y las soluciones que estamos poniendo en práctica para paliarlos. A continuación, describiré de forma sucinta nuestra aportación como miembros de la comunidad de expertos de ciberseguridad, ilustrada con un ejemplo de aplicación al área de la defensa. Terminaré mi intervención con las conclusiones y una propuesta de línea de acción.

Como la mayoría de ustedes saben, Indra es una empresa multinacional española de tecnología, con soluciones y servicios orientados a diferentes mercados tales como la energía, las telecomunicaciones, el transporte, la banca, las administraciones públicas, la sanidad, así como la defensa y la seguridad por citar los más relevantes. La actividad internacional es cada vez más importante, tenemos presencia en 45 países de los cinco continentes, y el 60% de nuestras ventas procede del mercado exterior.

Es bien conocido que la industria, al igual que los organismos gubernamentales y los individuos particulares estamos siendo atacados no ya por los **hackers clásicos**, aquellos que sólo pretendían notoriedad, sino por auténticos cibercriminales y hacktivistas, con grandes intereses comerciales, económicos, políticos o estratégicos.

Así, mientras en los años setenta y ochenta la motivación era el reto de acceder a las nuevas tecnologías y romper las barreras de control de entrada de los sistemas como mero entretenimiento, los noventa trajeron los primeros mercenarios, ***"Hackers",*** que robaban información, identidades, defraudaban telemáticamente, espiaban y otras actividades similares.

Como los ciclos se acortan, estos últimos años nos han traído cibercriminales organizados y profesionalizados, con motivaciones políticas o estratégicas.

Y entre toda esta variedad de tipologías que convive y se entrecruza hoy en el ciberespacio, vemos que actualmente abundan unos nuevos actores de gran trascendencia que no son otra cosa que **hackers patrocinados por los estados**, o si ustedes lo prefieren **estados reconvertidos en *hackers***.

Como empresa tecnológica que somos, con el condicionante además de ser una empresa de Defensa con más de diez años de experiencia en el campo de las tecnologías de ciberseguridad, nos enfrentamos a una doble vertiente, que hace que por una parte seamos objeto importante de ataques, y por otra formemos parte de la comunidad de expertos en tecnologías de ciberseguridad. Esta dualidad nos permite tener una visión completa y una experiencia creciente que aprovechamos para apuntar algunos de los retos tecnológicos que se van a afrontar en los próximos años, con el fin de provocar en un entorno como en el que hoy nos encontramos, el correspondiente debate, que a buen seguro será enriquecedor para todos.

Abordaré a continuación la primera de las vertientes el riesgo que los ciberataques suponen. Si me permiten la simplificación, un riesgo viene determinado por su naturaleza, su impacto, probabilidad de ocurrencia, continuidad y/o frecuencia.

Según su naturaleza, podemos categorizar los riesgos del ciberespacio de acuerdo a la siguiente división:

- Perturbación, o ataques contra la continuidad o disponibilidad de los sistemas que controlan el servicio.
- Robo o fuga de información sensible.
- Falseamiento o modificación de la información, para debilitar la integridad y fiabilidad de la misma.

Todo ello sin olvidar el último parámetro clave en la valoración de riesgos, la probabilidad de ocurrencia, su continuidad e impacto en la capacidad operativa de nuestros sistemas. Hasta ahora dicha probabilidad ha sido baja, sin embargo, las reglas del juego están cambiando.

¿Cuál es la razón principal de la proliferación de este tipo de actividades?... bastante evidente. En el ciberespacio, la ventaja está del lado del atacante: atacar una red es mucho más fácil que defenderla. Las razones son diversas, pero entre ellas se podría destacar la enorme desproporción que existe entre el esfuerzo necesario para un ataque cibernético, amparado en el anonimato y con la ventaja de elegir momento y objetivo, y el necesario para la protección de los sistemas; esto podrá cambiar con el tiempo, algún día en el ciberespacio podríamos tener el equivalente de la guerra de trincheras, donde el defensor encuentra una ventaja natural, pero no parece que esto se vaya a producir en el corto plazo.

Permítanme un ejemplo bastante ilustrativo, la media de muchos de los virus y ataques que sufrimos todos los días no requieren más de unas decenas de líneas de código. Por el contrario,

el software de seguridad que hace frente a estas amenazas, desarrollado en los últimos años, representa millones de líneas de código. **No** nos enfrentamos contra amenazas que simplemente comprometen nuestros sistemas informáticos, nos enfrentamos a **amenazas reales que ponen en peligro nuestros sistemas físicos incluyendo nuestros sistemas militares**, en definitiva ponen en peligro nuestras infraestructuras críticas, sea cual sea su naturaleza.

La importancia y los desastrosos efectos que producirían estos ataques obligan a adoptar medidas, desarrollar mecanismos y arbitrar soluciones capaces de neutralizarlos o, al menos reducir sus efectos a límites aceptables.

Esta característica, unida al hecho de que el ataque puede provenir de las más diversas fuentes, obliga a reforzar las acciones necesarias para llevar a cabo una adecuada acción conjunta de neutralización.

Además, tenemos que tener presente que:

- El medio ya no es sólo físico, sino virtual y no sólo natural sino también artificial
- La amenaza no es sólo cinética y tangible, sino también cibernética e intangible
- No existe el concepto clásico de fronteras y límites de influencia
- No existen barreras de distancia ni temporales
- La velocidad de desarrollo de acontecimientos se ha acelerado hasta el límite de haber alcanzado otro orden de magnitud

Pasaremos a continuación a describir brevemente, y sólo a modo de ejemplo, algunos aspectos prácticos que ilustran lo mencionado hasta ahora de forma conceptual y que en sí mismos constituyen retos importantes que debemos afrontar.

Comenzaremos por el concepto de **"*Big Data*".** En las últimas semanas, hemos podido ver y leer en las noticias que organismos como la **NSA** están capturando toda la información a la que tienen acceso, siendo almacenada para ser tratada posteriormente y que pueda servir de base de análisis que permita, en principio, únicamente la anticipación a la comisión de delitos o de ayuda al esclarecimiento de otros. Este concepto de **TIA, *Total Information Awareness*,** conlleva prácticas que derivan en el almacenamiento de ingentes cantidades de información, lo que ya en si mismo constituye un reto, ya que presupone la capacidad de proceso y análisis de una cantidad de información hasta ahora desconocida.

Además, este tipo de iniciativas plantean varios problemas:

1. Provocan la necesidad de un cambio tecnológico. Tecnologías que hasta la fecha eran "punteras", ahora ya no sirven, teniendo por lo tanto la necesidad de desarrollar las nuevas capacidades de "Big Data", ya que tratar de adecuar las herramientas y arquitecturas existentes a estos nuevos conceptos es complicado, si no imposible a fecha de hoy. Se trata en definitiva de una nueva forma de hacer las cosas frente a los sistemas

actuales, que trabajan bajo el principio de "sólo guardar lo importante, descartando lo demás", lo que lleva implícito que se debe saber de antemano lo que es importante.

2. Estas iniciativas implican además una dudosa frontera con la legalidad. La controversia está servida, y esto nos recuerda a la famosa frase *"big brother is always watching"* que George Orwell inmortalizó en su novela 1984.

3. Se produce un incremento significativo del coste de los sistemas.

4. Por otro lado, la mayor experiencia en conceptos y herramientas de ***"Big Data"*** está en las empresas de redes sociales, aunque de hecho la tecnología proviene del mundo académico. Esto causa un problema para muchas empresas, con especial acento en Europa, dado las redes sociales tienen su origen en los EE.UU.

5. Las soluciones de ***"Big Data"*** tardarán todavía unos años en adaptarse al mercado de seguridad, ya que las existentes proceden fundamentalmente del entorno del marketing.

¿Puede ser el "Estado" el enemigo?

Un fenómeno importante que me gustaría destacar es que la industria ha estado defendiéndose contra ***hackers, hacktivistas***, **cibercrimen**, pero nunca hasta ahora, se ha tenido que enfrentar a un combatiente tan potencialmente poderoso como son los cibercomandos de los Estados. Las Empresas nunca habían tenido que defenderse contra ataques protagonizados por las fuerzas armadas de otros estados. Hasta ahora la ciberseguridad ha sido una cuestión de buenas prácticas, tecnologías y sentido común, pero cuando el atacante tiene los recursos de un estado nos encontramos con un salto cuántico de consecuencias todavía impredecibles.

Implica que o bien las empresas acometen grandes inversiones para defenderse o se establecen nuevas formas de involucración del propio estado en la defensa de los intereses de sus empresas nacionales.

El ciberespacio es un **"*global common*",** y desde esa perspectiva, necesita de una respuesta global. No vale una respuesta local y específica para un problema global y genérico. Por esa razón la cooperación internacional con gobiernos aliados y organizaciones de ámbito supranacional es esencial.

Otro problema al que nos enfrentamos es la presencia de Internet en casi todos los dispositivos.

En la actualidad, la **"internetización"** creciente de cualquier dispositivo presente en nuestros hogares o lugares de trabajo es ya un hecho. Así una impresora, por poner un ejemplo, es hoy en día un ordenador Linux. Se imaginan que hubiera un "***rootkit***" para estas impresoras que las convirtieran en plataformas de ciberespionaje, podríamos encontrarnos con que todos los documentos que pasaran por ellas se subieran a un servidor en internet, ¿y si además funcionara para escanear la red y lanzar ataques? Y esto que podemos imaginar para impresoras, por qué no reescribirlo para cualquiera de los dispositivos que actualmente encontramos conectados a internet, o por qué no para todos aquellos que en breve lo estarán.

Telefono Voz IP, tableta Android, frigorífico o TV inteligente... Cuando haya que monitorizar y defenderse contra todos estos dispositivos que tienen o tendrán conectividad directa o indirecta a la red, nos encontraremos sin duda ante un nuevo reto tecnológico, organizativo y administrativo. Antes era fácil decir 'no conectes eso aquí', pero cuando está conectado todo hay que repensar las arquitecturas tradicionales. Ya no valen los modelos de arquitecturas actuales.

Y si a todos estos dispositivos añadimos los sistemas de control industrial, como los **SCADA**,nos encontramos ya de hecho en una nueva era donde el paradigma del ciberespacio lo envuelve todo y los conceptos holísticos de la seguridad se convierten en indispensables.

Otro reto para las empresas es lo que se conoce como "BYOD"

Una práctica actualmente muy habitual y que seguro que les resulta familiar es la de **"*Bring Your Own Device*".** Está de actualidad porque representa una ventaja competitiva para las empresas, pero a su vez supone un reto en tanto en cuanto implica adoptar medidas de seguridad para unos medios sobre los que no se tiene control.

Está de moda porque no tiene sentido que si una persona tiene por ejemplo, un ***tablet*** de última generación, y está dispuesta a utilizarlo en su entorno de trabajo ahorrando costes a la empresa, ésta le prohíba su uso. Parece más razonable que se plantee como reforzar las medidas de seguridad, y que así esta tendencia pueda ser efectiva en nuestras organizaciones.

Sin embargo sabemos que en la **operación Aurora** se consiguió entrar en una red de una empresa, infectando, con un ataque tipo ***watering hole***, a un desarrollador que trabajaba desde casa. Cuando se conectó a la red interna, se cerró el ciclo de la **APT (Advanced Persistent Threat).**

Pero permítanme explicar de forma simple, para aquellos no familiarizados con estas tecnologías, en qué consiste un ataque del tipo ***watering hole***. Imagínense que queremos atacar un centro estratégico y que algunos de sus miembros más relevantes pertenecen a un **club** (de golf por ejemplo). Qué pasaría si infectamos con un determinado ***malware*** la web de este club. Es seguro que estos miembros se terminarán conectando a la web de su club favorito y de esta forma terminarían también infectados. Cuando se vuelvan a conectar con sus terminales a sus centros de trabajo tendremos nuestro ***malware*** dentro de los sistemas del objetivo de nuestro ataque y a partir de aquí pueden imaginarse el resto.

En estos nuevos escenarios donde "todo el mundo" trae su ***Smartphone, Tablet, iWatch*** o lo que sea, y quiera conectarse para usar recursos internos de las empresas y organismos donde trabajan, hay que cambiar el paradigma de sólo defender sistemas. Es preciso establecer medidas especiales para defender aquellos datos que consideremos estratégicos. Les aseguro que el tema es objeto de debate en mi empresa estos días, como seguro lo será en varias de las suyas.

¿Cómo abordamos en la empresa estos nuevos desafíos?

Los nuevos paradigmas son la seguridad activa y la gestión dinámica del riesgo

Hace tan sólo unos años se trabajaba sobre la hipótesis de la seguridad estática que implicaba que con un ***firewall*** y un ***antimalware*** actualizado, y un poco de suerte, podrías estar seguro.

Sin embargo, ahora se sabe que:

1. El antimalware no es capaz de detectar los ataque dirigidos y diseñados para una instalación concreta.

2. Todo el mundo es objetivo, o puede serlo, de alguien, en algún momento.

3. Hay que proteger los sistemas pero también hay que implantar medidas específicas para proteger la información con técnicas DLP (Data Lost Protection). Los datos vitales se protegen de una forma especial

4. Es preciso un plan de respuesta activa ante incidentes.

5. Hay que emplear técnicas de defensa en profundidad, barreras de seguridad distintas, con diferentes mecanismos de autenticación, segmentación de redes, diferentes tecnologías, …

Todo ello nos lleva a la implantación de sistemas complejos de monitorización, análisis y reacción rápida, acompañados de herramientas de conciencia situacional y una sofisticada gestión dinámica del riesgo.

Esto nos debe llevar a Sistemas Robustos y de "*mision completion*" o garantía de cumplimiento de misión

El incremento del interés por las tecnologías de la información ha tenido una consecuencia inmediata: el creciente desarrollo de las industrias dedicadas a las tecnologías de la información y su cada vez mayor implicación en todo tipo de actividades y procesos. Hoy podemos afirmar que desde las grandes corporaciones de la banca, hasta la gestión de las redes eléctricas o de ferrocarriles, pasando por los sistemas militares de mando, control e información, todos basan sus actividades en programas informáticos concebidos y desarrollados teniendo muy presente que han de estar dotados del máximo nivel de inviolabilidad.

Esta nueva era del ciberespacio como exponente de crecimiento y de conflictos, ha puesto de moda el concepto de ***resiliencia***. Las tecnologías ***cloud*** **y nube privada** permiten pensar en sistemas altamente robustos que pueden cumplir sus tareas mientras están siendo atacados. Cuando se cae un sistema, hay otro, quizás en otro continente, esperando y listo para continuar. El reto al que nos enfrentamos es la adecuación de los sistemas actuales para funcionar en estos entornos altamente paralelizados.

Con las herramientas de virtualización es posible mover sistemas tradicionales a estos entornos para darles una robustez que antes no tenían. Este concepto de sistemas se denomina sistemas con capacidad de ***'mission completion'*** aunque estén siendo atacados. Es decir, arquitecturas especialmente diseñadas para cumplir su misión aunque parte de estructura pueda ser dañada.

No quiero dejar de comentar, llegado a este punto, el problema que las empresas tienen que abordar, desde la perspectiva de la responsabilidad social corporativa, de reconocer que estamos siendo atacados, y de denunciarlo.

Una vez hemos repasado los retos a los que la industria se enfrenta, pasamos a continuación a tratar la segunda de nuestras vertientes, la de formar parte de la comunidad de expertos en tecnologías de ciberseguridad, y la aplicación de estas tecnologías al entorno de la defensa.

Ya he comentado anteriormente que represento una empresa tecnológica que lleva ligada al mundo de las tecnologías de seguridad de la información desde hace más de 10 años. Contamos con un equipo de más de 250 profesionales en la materia, y estamos ayudando a instituciones públicas y privadas, de diferentes sectores, tanto en actividades de servicios preventivos, como reactivos y correctivos.

Sin embargo sí quiero, en mi condición de responsable de Defensa en Indra, poner énfasis en la importancia que esta experiencia tiene para la construcción de la Ciberdefensa Nacional. Desde una perspectiva de empresa, no es más que un movimiento lógico de diversificación, que ya han emprendido también otras empresas multinacionales del sector, por el que aspiramos a aplicar productos derivados de los actuales a un cliente como el Ministerio de Defensa, que siempre ha sido uno de nuestros clientes prioritarios, y con el que hemos mantenido una relación muy estrecha que se remonta a décadas de trabajo conjunto.

El desafío no está tanto en su tamaño, trabajamos en el ámbito de la ciberseguridad con muchas grandes corporaciones, ni en su naturaleza pública, porque tenemos mucha experiencia en nuestro trato diario para este mismo ámbito con otras áreas de la administración, sino en la adaptación de estos conceptos y productos a las necesidades específicas de la Defensa.

Desde la óptica de las Operaciones de Defensa, el Ciberespacio, como quinto escenario de operaciones tras los cásicos de Tierra, Mar y Aire y el no tan clásico, pero asumido ya como normal, del espacio, plantea una serie de singularidades que requieren una profunda reflexión así como una revisión de la doctrina clásica. La adaptación de las estrategias tradicionales a este nuevo escenario permite diferenciar tres tipos de operaciones:

1. **Operaciones defensivas con efecto cibernético.**
   Se considera efecto cibernético la manipulación, disrupción, denegación, degradación o destrucción de cualquier elemento de un sistema de información ya sea físico o virtual.
   Una operación defensiva con efecto cibernético es aquella ejecutada en el ciberespacio y encaminada a producir un **efecto cibernético en redes ajenas** con el fin de defenderse o protegerse frente a una amenaza inminente, ataque en curso o actividad maliciosa contra los propios intereses.

2. **Contramedidas defensivas no intrusivas**
   Se diferencian de las anteriores en que la operación se lleva a cabo en redes propias o con la debida autorización, y producen un efecto cibernético mínimo. Por ejemplo, podría degradarse o interrumpirse un servicio o segmento de red para mitigar el impacto de un ataque.

3. **Operaciones ofensivas con efecto cibernético**
   Son operaciones encaminadas a producir un efecto cibernético en redes ajenas sin propósitos defensivos, de recolección de información o inteligencia.

¿Donde está la mayor diferencia respecto a nuestra actividad en el mundo civil? Mientras no existe una diferencia conceptual importante entre la protección cibernética de una instalación militar y la de una infraestructura crítica civil,no somos ajenos a que una **ciber-operación** tipo, puede implicar el uso de **ciberarmas**, siendo una **ciberarma un *malware* y elementos adicionales diseñados específicamente para causar un efecto cibernético que otorgue superioridad en un conflicto.**

Debido a la rápida evolución de la tecnología y a la propia naturaleza de las ciberarmas es imprescindible conocer la curva de devaluación y el carácter temporal del valor estratégico de las mismas:

- Con una inversión mucho menor que lo que requiere el armamento tradicional pueden aportar una ventaja militar muy significativa en un conflicto.

- Sin embargo, una ciberarma se diseña típicamente para ser dirigida a un sistema de información y configuración muy concretos, los cuales evolucionan muy rápidamente.

- Ello, sumado a unos plazos de desarrollo no inmediato, hace que deba planearse adecuadamente la inversión y desarrollo de una ciberarma con su uso o como apoyo a un conflicto armado.

Para aumentar la eficacia del **ciberarmamento** es necesario disponer de un **sistema de cibercombate** adecuado, que ofrezca un sofisticado **cuadro de mando y control** así como de la capacidad de adaptar o evolucionar ciberarmas en base a experiencias y capacidades anteriores. Ello reduciría drásticamente los tiempos necesarios para producir nuevas ciberarmas eficaces en un conflicto armado que deba desarrollarse en un corto plazo.

Estamos afrontando nuevos retos que requieren tomar decisiones adaptadas a las particularidades de este nuevo escenario, por lo que será importante tomar en consideración que los procesos que gobiernan la seguridad son procesos de mejora continua, donde la **evolución en espiral** es una buena práctica que nos debe permitir avanzar aprovechando las lecciones aprendidas en cada etapa.

En tanto en cuanto, como ya he comentado, represento a una empresa con una presencia importante en el ámbito de la defensa y la simulación, me he permitido abordar esta parte de mi intervención de hoy describiendo un ejemplo simulado de operación convencional comparada con una en el ciberespacio. Imaginemos entonces el planeamiento y la ejecución de una operación tradicional y veamos las similitudes y diferencias con una operación en el ciberespacio

Así, el ciclo clásico de Mando y Control, mediante el cual se planifican y conducen las operaciones es fundamentalmente idéntico, cambiando únicamente los medios puestos en juego, así como las herramientas de apoyo utilizadas. El Planeamiento de cualquier operación parte desde la información de inteligencia que permite ubicar la operación dentro de un

escenario y contexto lo más conocido posible. Dentro de este contexto, y en función de la misión a llevar a cabo, entra en juego la logística para seleccionar los medios y el personal involucrado en la operación, ya sea sobre el terreno o en apoyo de la misma. Dichos medios son utilizados según diferentes alternativas en una fase clave del planeamiento,de manera que se evalúen diferentes derroteros por los que pueda discurrir la operación y puedan valorarse diferentes niveles de riesgo y de probabilidad de éxito. En esta fase, resulta clave la contribución de las secciones de inteligencia y las de operaciones, las cuales, atendiendo a unas determinadas reglas de confrontación, simulan el curso del enfrentamiento y permiten anticipar el curso real que tendrán las operaciones sobre el escenario.

Una vez determinadas las diferentes líneas de acción, se selecciona la adecuada y se genera la orden que fluye hacia la organización a través de la cadena de mando. La organización se moviliza en consecuencia y se informa al mando sobre el curso de la operación durante el proceso de conducción para mantener una actividad de evaluación de resultados constante y abordar, en caso de que los acontecimientos lo recomienden, un replaneamiento y nuevas órdenes orientadas a adaptar la operación y a maximizar la probabilidad de éxito con el menor riesgo posible.

Este es en síntesis, el ciclo de mando y control de las operaciones militares que seguro conoce muy bien buena parte de la audiencia de esta ponencia.

La irrupción de las nuevas tecnologías tanto en el terreno de las herramientas involucradas como en el de los medios puestos en juego no ha venido a modificar en lo sustancial esta doctrina. Los avances en las comunicaciones, han incrementado la rapidez y la eficiencia en el flujo de órdenes y la coordinación entre los procesos. La paulatina introducción de los medios informáticos ha posibilitado un manejo más eficiente de recursos básicos como Mapas, Bases de Datos, Herramientas Gráficas y de Documentación. Asimismo, la introducción de nuevas arquitecturas como la ***Network Centric Warfare***, han cambiado la filosofía de acceso, diseminación y explotación de la información.

Sin embargo, ninguno de los elementos anteriores ha sido capaz de dar un giro radical al concepto doctrinal de las operaciones dado que en lo esencial los fundamentos y conceptos que las rigen no han cambiado.

Hagamos ahora abstracción a un nuevo escenario de la confrontación, el Cibersespacio, y plateemos un ejemplo clarificador basado en una operación militar clásica de cancelación de comunicaciones, infraestructuras críticas de suministro de energía e inhabilitación de centros de decisión.

Resulta fácil imaginar, en el concepto clásico, una operación en la cual se planifiquen ataques aéreos destinados a la supresión de las defensas, y la interrupción de vías de comunicaciones terrestres, puentes, vías de ferrocarril e infraestructuras de generación y transporte de energía.

Los medios puestos a disposición de la operación serían medios aéreos adecuados con toda la logística de apoyo necesaria: combustible, personal, bases aéreas, reabastecimiento en vuelo, pilotos, armamento, comunicaciones...

Los datos de inteligencia necesarios para el planeamiento estarían conformados por la ubicación de las defensas, de los objetivos, la meteorología, la visibilidad, la hora de la operación, el entorno.

La fase de confrontación evaluaría diferentes variantes de oleadas de ataque, perfiles de vuelo, número de atacantes, simultaneidad, reacciones previsibles, porcentajes de éxito, efectos sobre las defensas.

Luego se seleccionaría una línea de acción, se generaría la orden y se dispondrían los preparativos con antelación suficiente cuidando de la vulnerabilidad e integridad de la información y manteniendo al mando puntualmente informado sobre los acontecimientos.

Finalmente se llevaría a cabo la operación con sus correspondientes planes y medios de contingencia y vamos a suponer que, como colofón tiene éxito y se consigue la destrucción de las vías de comunicación planificadas tanto terrestres como férreas. Se afecta a la capacidad de generación de energía y se minimiza, la capacidad del mando para la toma de decisiones y la gestión.

El escenario planteado tendría gran complejidad logística y un desarrollo en el tiempo de varias semanas o meses con una demanda de medios muy alta. Probablemente, en caso de éxito, únicamente representaría el preámbulo de una operación de mayor calado y todavía mayor complejidad.

Llevemos ahora el tema al terreno de la Ciberdefensa… Mismos objetivos y mismos efectos. La fase de planeamiento tendría una profundidad similar. Se captarían datos de inteligencia cuya procedencia sería la red y el acceso potencial a la evolución del escenario sería mucho más ágil, fiable y puntual. La definición de medios sería, de largo, más simple y concentrada, implicando únicamente ciberarmamento, ***malware*** y acceso a comunicaciones. La evaluación de los efectos, sería asimismo mucho más fiable por predictiva y analizable mediante simulación y los medios involucrados en la operación mucho menos distribuidos en cuanto a los órganos de decisión y deslocalizados en cuanto a la ejecución, pero extremadamente accesibles.

Desencadenado el ataque, las vías de comunicación de datos y líneas telefónicas resultan extremadamente vulnerables a un ciberataque por lo que una correcta planificación garantiza su colapso y desestabilización.

En cuanto a las comunicaciones terrestres, basta con actuar sobre la gestión de señalizaciones, semáforos, gestión de tránsito por vías férreas y terrestres, sistemas de información de aeropuertos y sistemas de control de tráfico aéreo para colapsar completamente a un país con difíciles vías de recuperación inmediata.

Las fuentes de generación de energía, así como sus canales de distribución, son también vulnerables a agentes externos de naturaleza cibernética en sus puntos y elementos de control, por lo que se hace posible imaginar una actuación en este ámbito para desestabilizarlas.

En este estado, las vías de defensa y los canales de decisión se tornan en ineficientes y el efecto buscado se consigue de un modo seguro, eficiente en coste y con un mínimo daño colateral. En este caso, para el mismo efecto, el período de planeamiento y ejecución de la misión puede ser de días.

Tal y como queda reflejado en el trasfondo del ejemplo construido, en un escenario de operaciones Cibernético, los conflictos se dirimen desde un contexto espacial absolutamente alejado de lo clásico, desde una oficina o un centro de cálculo, los medios puestos en juego son absolutamente alejados de lo convencional, incluso sin entidad física, los aspectos temporales son de otro orden de magnitud e incluso las líneas de acción y la anticipación del resultado son mucho más sensibles al uso de las herramientas de simulación para su análisis fiable.

No obstante, los resultados, como pueden derivarse asimismo del ejemplo, pueden ser igualmente cinéticos y, si me lo permiten, tan cruentos como los resultantes de un ataque convencional.

De todo lo anterior, aparece la necesidad de adaptar conceptos clásicos de las Operaciones de Defensa a este nuevo escenario. De esta forma:

- El Armamento deviene en Ciberarmamento
- Los Ejércitos en Ciberejércitos
- Los campos de batalla en Ciberespacio
- La disuasión en Ciberdisuasión

Un largo etcétera como, ciberterrorismo, ciberespionaje, cibercrimen, ciberefecto, ciberoperación, ciberinteligencia, ciberactivismo, y muchos otros nuevos términos que se acuñan cada día.

Como de retos hablamos, sinceramente creo que nos enfrentamos a algunos de los más grandes aparecidos en las últimas décadas. Como hemos visto, e incluso insistido a lo largo de esta presentación, la ciberseguridad representa un nuevo escenario en el que, si bien se parte de una experiencia sólida, vemos que el ritmo de evolución de los acontecimientos nos lleva a plantear que casi todo está por ser definido.

Y este escenario, que sin ninguna duda es sumamente inquietante desde un punto de vista intelectual, conlleva también la necesidad de afrontar las oportunidades que se esconden tras los múltiples retos que hemos enumerado.

Desde la óptica industrial tenemos ante nosotros la obligación y la responsabilidad de no perder un tren que está partiendo y que debe permitir a la industria española estar entre los líderes tecnológicos de un mercado emergente. Nosotros creemos en ello y estamos poniendo los medios para ser uno de los exponentes en el desarrollo de esta tecnología.

Ya para terminar, me gustaría recalcar que para que estos retos que afrontamos desde la industria puedan tener éxito, es indispensable que sean acompañados por unos esfuerzos similares desde el lado de la Administración.

Para los Estados, los retos son más importantes si cabe, ya que suponen la necesidad de mantener, en este contexto de amenazas cibernéticas, el actual grado de desarrollo del estado del bienestar, basado en el desarrollo normativo, tecnológico e industrial. Una sociedad moderna no se concibe sin un grado avanzado de seguridad y en las sociedades del futuro, una pieza fundamental de la seguridad debe ser la Ciberseguridad. Por ello, desde esta tribuna animamos al rápido desarrollo de la Estrategia Nacional de Ciberseguridad en todas sus vertientes, que nos garantice un futuro compatible con el progreso.

Sin embargo, no es sólo esa faceta la que a nosotros como industria, nos afecta. Desde las empresas, estamos trabajando en el mercado de la seguridad para que se constituya un importante vector de crecimiento de nuestra industria, pero estamos convencidos de que este esfuerzo será inútil si no va acompañado por un esfuerzo similar de desarrollo a nivel estatal. En las circunstancias actuales, donde la exportación representa la base del crecimiento de nuestras empresas, la confianza internacional en nuestras soluciones sólo será posible si logramos un grado de desarrollo nacional que nos permita mostrarlo como bandera y referencia en el exterior.

En resumen:

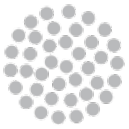
- La ciberseguridad plantea una serie de amenazas y retos, que van acompañados de oportunidades que no se deben ignorar, y que deben ser gestionadas de forma adecuada.
- Las empresas no pueden luchar contra la ola de conectividad que vivimos, sino que tienen que gestionarla adecuadamente desde el punto de vista de la seguridad.
- La Administración, como la comunidad internacional, tienen una responsabilidad ineludible en la provisión de ciberseguridad.
- Un problema global sólo puede tener una solución global.
- Es hora de pasar de la planificación a la acción, y hay que pensar en espirales evolutivas.
- La Administración, los Cuerpos y Fuerzas de Seguridad del Estado y las Fuerzas Armadas no puede quedar fuera de este movimiento.

Muchas gracias a todos por su atención y paciencia. Quedo ahora a disposición de ustedes para cualquier pregunta o comentario que quieran efectuar.

XXVI Cursos de Verano 2013. Universidad Complutense

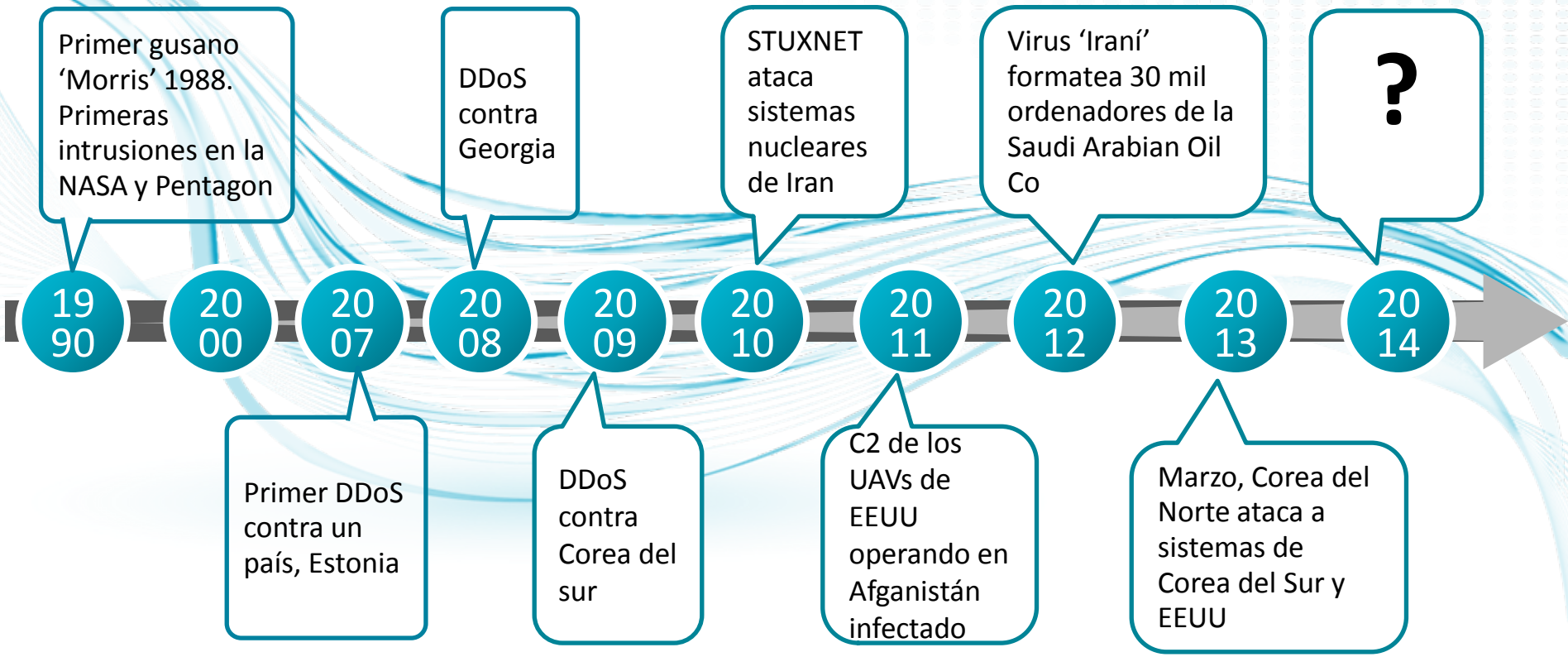
Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio

LOS RETOS TECNOLÓGICOS E INDUSTRIALES DE LA CIBERSEGURIDAD



indra

CRONOLOGÍA DE LOS CIBERATAQUES



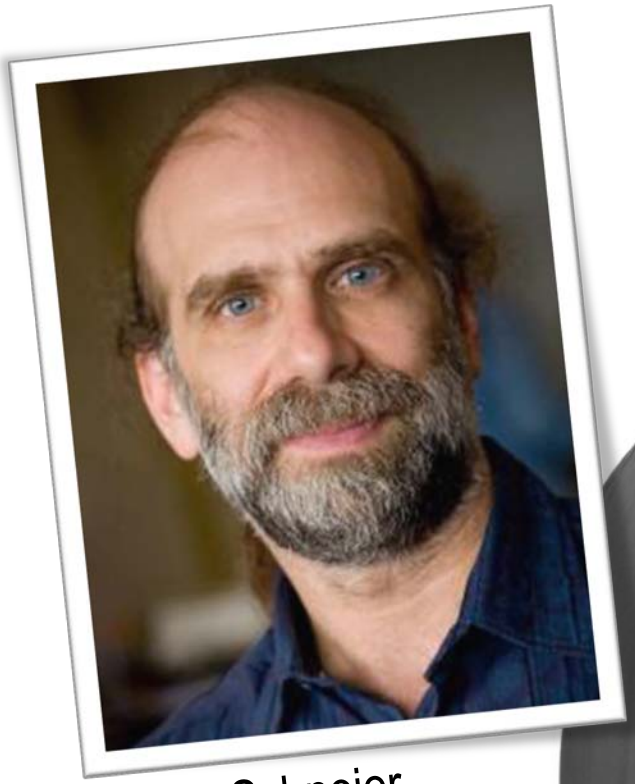
LAS NUEVAS AMENAZAS

Según su naturaleza, podemos categorizar los riesgos del ciberespacio de acuerdo a la siguiente división:

- **Perturbación, o ataques contra la continuidad o disponibilidad**
- **Robo o fuga de información sensible**
- **Falseamiento o modificación de la información**

EL BALANCE DE PODER

"En el ciberespacio, el balance de poder está en el lado del atacante. Atacar una red es más facil que defenderla…"



Bruce Schneier
Schneier on Security

EL USO DE BIG DATA

El General Keith Alexander, jefe del Cibercomando Estadounidense y la NSA

EL ESTADO COMO ENEMIGO

BBC NEWS TECHNOLOGY

12 October 2012 Last updated at 10:38 GMT

US prepares first-strike

Cyber-attacks could inflict as much damage on the US as the physical attacks on 11 September 2001, the US defence secretary has warned.

Leon Panetta said the country was preparing to take pre-emptive action if a serious cyber-attack was imminent.

The New York Times

Panetta Warns of Dire Threat

By ELISABETH BUMILLER and THOM SHANKER

Published: October 11, 2012

Defense Secretary Leon E. Panetta warned Thur... States was facing the possibility of a "cyber-Pear... increasingly vulnerable to foreign computer hac... dismantle the nation's power grid, transportatio... networks and government.

REUTERS EDITION: U.S.

Exclusive: Insiders suspe... cyber attack

By Jim Finkle

Fri Sep 7, 2012 4:52am EDT

(Reuters) - One or more insiders with high-level access are suspected of assisting the hackers who damaged some 30,000 computers at Saudi Arabia's national oil company last month, sources familiar with the company's investigation say.

CNN

Home Video World U.S. Africa Asia Europe Latin America Middle East

ENTREVISTA DIGITAL ¿Dónde invertir en Bolsa? Pregunta EN DIRECTO al experto de Atlas Capital Ignacio Cantos

EL PAIS

INTERNACIONAL

Estados Unidos y China, ante la primera ciberguerra fría

Obama firmó una orden ejecutiva la pasada semana que le otorga poderes especiales

ANTONIO CAÑO | Washington | 19 FEB 2013 - 20:06 CET 135

Archivado en: Barack Obama Guerra electrónica Ataques informáticos China Ciberactivismo Seguridad internet Asia oriental Activismo Guerra Estados Unidos Internet Norteamérica Asia Telecomunicaciones Conflictos América Comunicaciones

El presidente Barack Obama durante una intervención en Washington este martes. / JIM LO SCALZO (EFE)

La Casa Blanca describió este martes los reiterados ataques cibernéticos, que una investigación reciente vincula directamente con una unidad secreta del Ejército chino, como "un serio desafío para la seguridad y la economía de Estados Unidos", lo que es la señal de que una nueva guerra fría, en el desconocido e incontrolable espacio de Internet, ha comenzado entre las dos grandes potencias que se disputan la supremacía en el siglo XXI.

Sin acusar directamente a China, por

...nformático afecta a 30.000 ordenadores

...eares está a salvo del gusano Stuxnet

...stán a salvo, pero ha reconocido que ...adores dentro de su territorio y continúa ...deojuego, se trata de algo mucho más ...a no operaba correctamente por unos programas troyanos

...sta de los 'ciberataques' ...jército chino revela una ...la que pocos esconden

...dificio de la 'Unidad 61398'. | Foto: City8.com, via Mandiant

...iro Mejía (Efe) | Washington Comentarios

...tualizado jueves 21/02/2013 10:11 horas

...a revelación de identidades y 'modus operandi' de los miembros de la ...puesta unidad de 'hacking' más secreta del Ejército chino ha sido ...talada hasta el extremo y los expertos consideran que China ...

website hacked by Syria's Assad loyalists

Tue, Sep 4 2012

Exclusive: White House studying potential oil reserve

...ros socios

SERVICIOS

RSS?

OTROS IDIOMAS

ENGLISH

Algunos comentaristas se asombraron cuando, hace poco menos de un año, un alto funcionario del Ministerio de Defensa de Estonia, Mijaíl Tammet, le dijo a la BBC que ambas situaciones eran comparables.

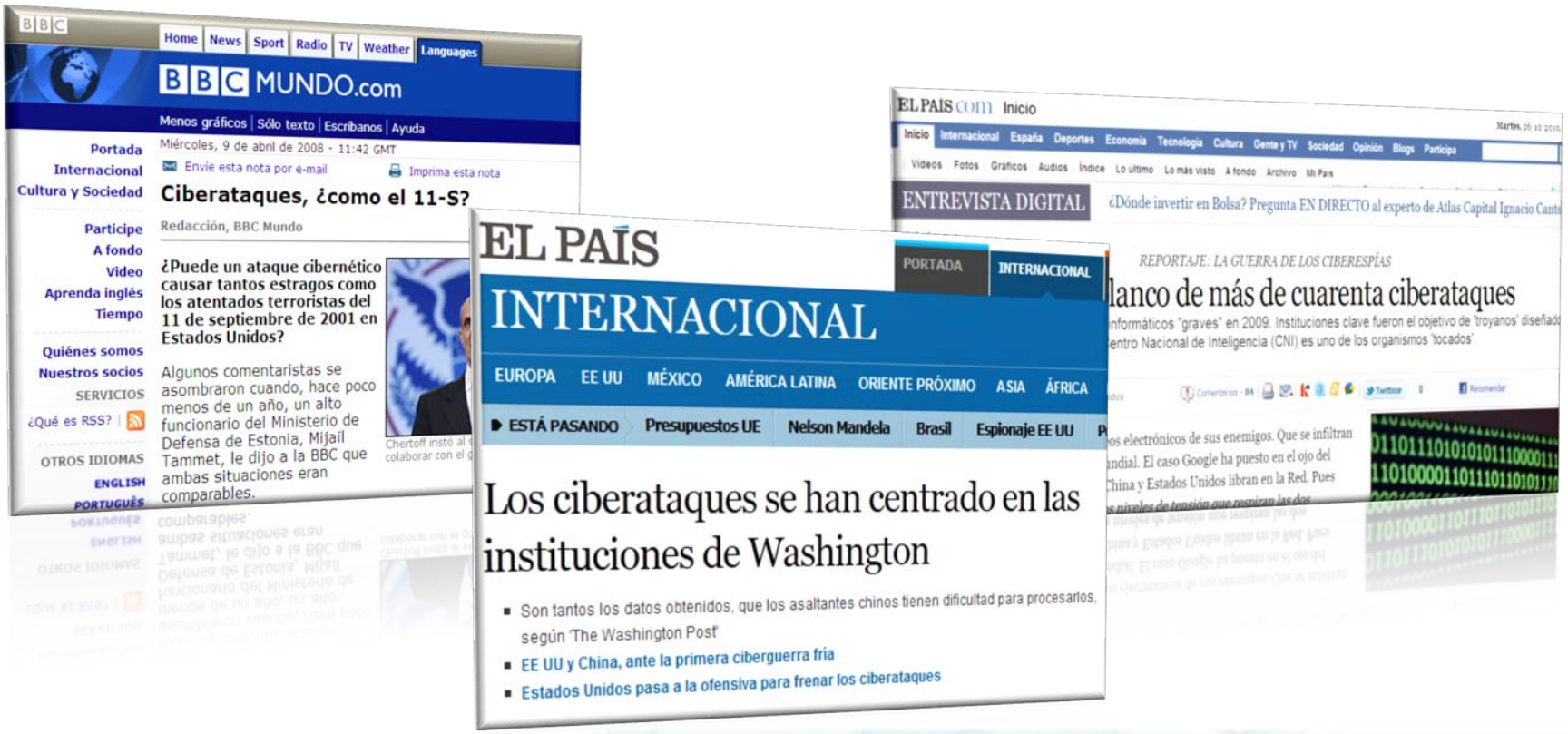
Chertoff instó al sector privado a colaborar con el gobierno.

LOS PARADIGMAS ESTÁN CAMBIANDO

El incremento de la dependencia de los Sistemas de Información

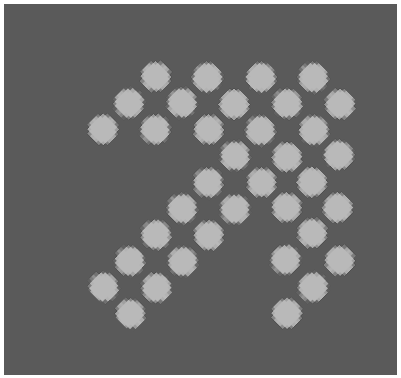
La complejidad de los medios TIC: Cloud Computing

Ciberguerra como una amenaza real



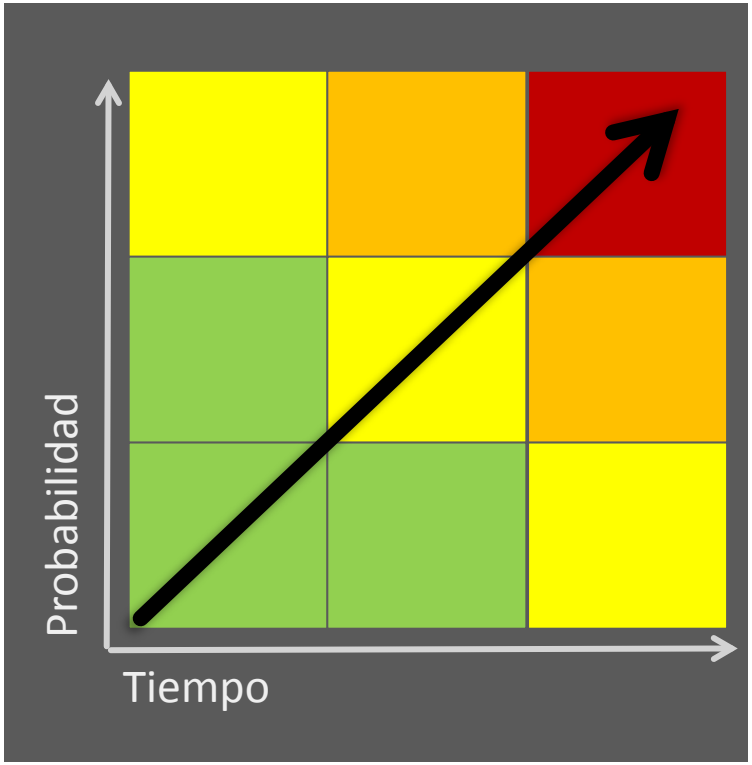
EVALUACIÓN DEL RIESGO

La probabilidad de ataques está aumentando



PROBA-BILIDAD EN AUMENTO

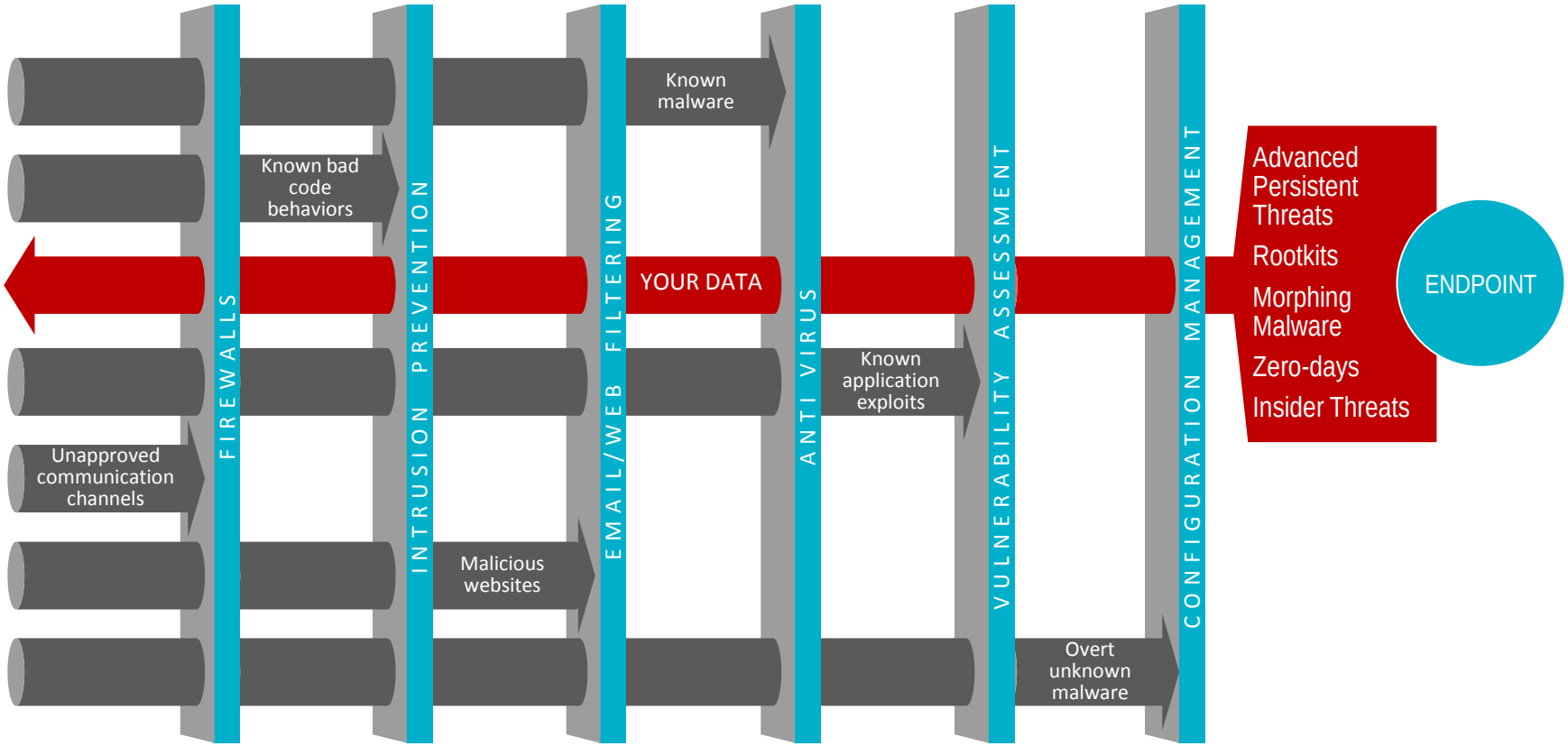
ALTO IMPACTO



Empresas atacadas

Empresas con presencia en Internet

DEFENSA EN PROFUNDIDAD



"La mentalidad de fortaleza no funciona en el Ciberespacio. No podemos protegernos detras de una Linea Maginot de cortafuegos….. Si permanecemos quietos durante un minuto nuestro adversario nos adelantará."

William Lynn, U.S. Deputy Secretary of Defense. January 2010

CAMBIOS EN LA DOCTRINA MILITAR

By Jim Wolf
WASHINGTON | Tue Feb 2, 2010 3:46am IST

Feb 1 (Reuters) - The U.S. Defense Department is putting cyberspace on a par with land, sea, air and space as a potential conflict zone, and developing new ways to operate there, a top-level Pentagon's strategy review said Monday.

Gobiernos y organizaciones internacionales han creado cibercomandos específicos para defenderse ante las amenazas emergentes

LAS CIBERARMAS

ABC.es | TECNOLOGÍA

ACTUALIDAD DEPORTES CULTURA VIAJAR GENTE&ESTILO TV VIDEO SALUD BLOGS

España Internacional Economía Sociedad Bodas Toros Madrid Ediciones Ciencia Medios Familia Defensa Opinión

TECNOLOGÍA / CIBERGUERRA

Descubren la mayor «ciberarma» de la historia del espionaje en internet

El virus Flame llevaba operativo 5 años en Oriente Medio, por lo que otras armas similares pueden estar ya en funcionamiento

J. F. A. / MADRID

Día 29/05/2012 - 09.16h

```
assert(loadstring(config.get("LUA.LIBS.table_ext")))()
if not __LIB_FLAME_PROPS_LOADED__ then
    LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSI
    flame_props SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTER
    flame_props INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.B
    flame_props BPS_KEY = "BPS"
    flame_props PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERV
    flame_props getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
            local l_1_0 = config.get
            local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
            return l_1_0(l_1_1)
```

ABC

Imagen de Flame, un virus malicioso utilizado como arma cibernética

http://www.bbc.co.uk/news/

News | Sport | We

BBC Mobile

NEWS 20 September 2011 Last updated at 10:56 GMT

Home UK Africa Asia-Pac Europe Latin America Mid-East South Asia US & Canad

Magazine In Pictures Also in the News Editors' Blog Have Your Say World Radio a

LATEST: China denies suggestions it may have been responsible for hacking attack on Jap

Japan defence hit by cyber attack

Japan's biggest weapons maker laur investigation into a cyber attack, bel first of its kind against the country's industry

E-mail hack attacks an 'epidemic'

Cyber-attack hits Lockheed Martin

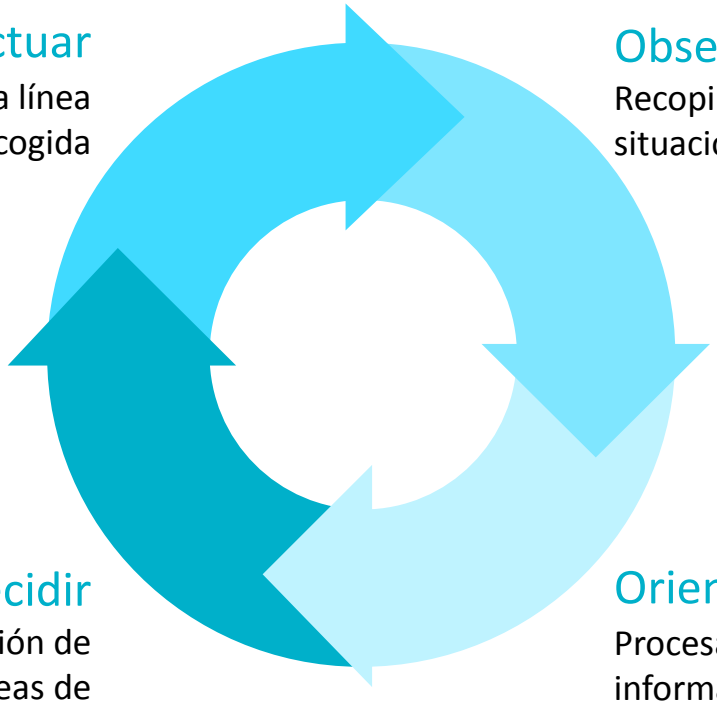
Cyber-sabotage tops secunty fear

Italy has debt rating cut by S&P

Italy's credit rating is cut by Standard and Poor's, but Prime Min Berlusconi says the move is based on "political considerations"

Greece bailout talks 'productive' In graphics: Deficits c

CICLO DE MANDO Y CONTROL (OODA)



Observar
Recopilación de la información de situación

Orientar
Procesamiento de la información y alcance de "conciencia de la situación"

Decidir
Evaluación y valoración de diferentes líneas de acción

Actuar
Ejecución de la línea de acción escogida

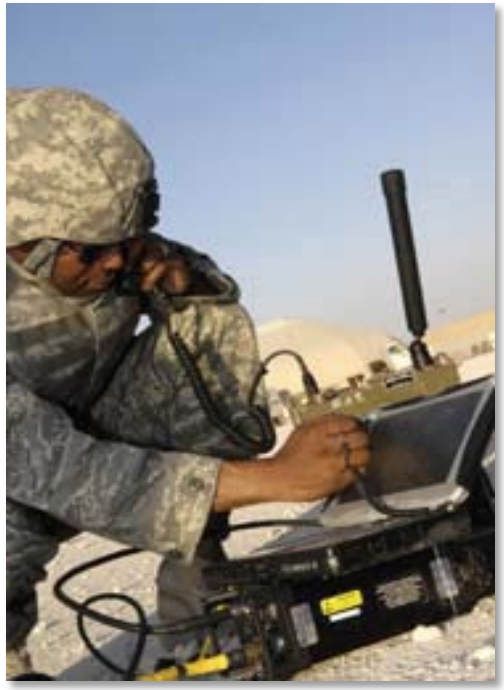
> "El Ciclo OODA se repite de forma cíclica con un periodo que debe adaptarse para no tomar decisiones en base a información que puede estar obsoleta (agilidad)."

FASES DE MANDO Y CONTROL

SISTEMAS MANDO Y CONTROL

Entorno complejo con un gran número y variedad de actores, múltiples roles y situaciones muy cambiantes o incluso impredecibles

Los tiempos de respuesta son clave, es necesario tomar decisiones en tiempo casi real



Las decisiones erróneas pueden tener un alto coste (humano, material)

Los Sistemas de Mando y Control tienen una fuerte dependencia del problema concreto en el que se aplican (Sistemas Terrestres, Aéreos, Entorno Marítimo, Anfibio, etc.)

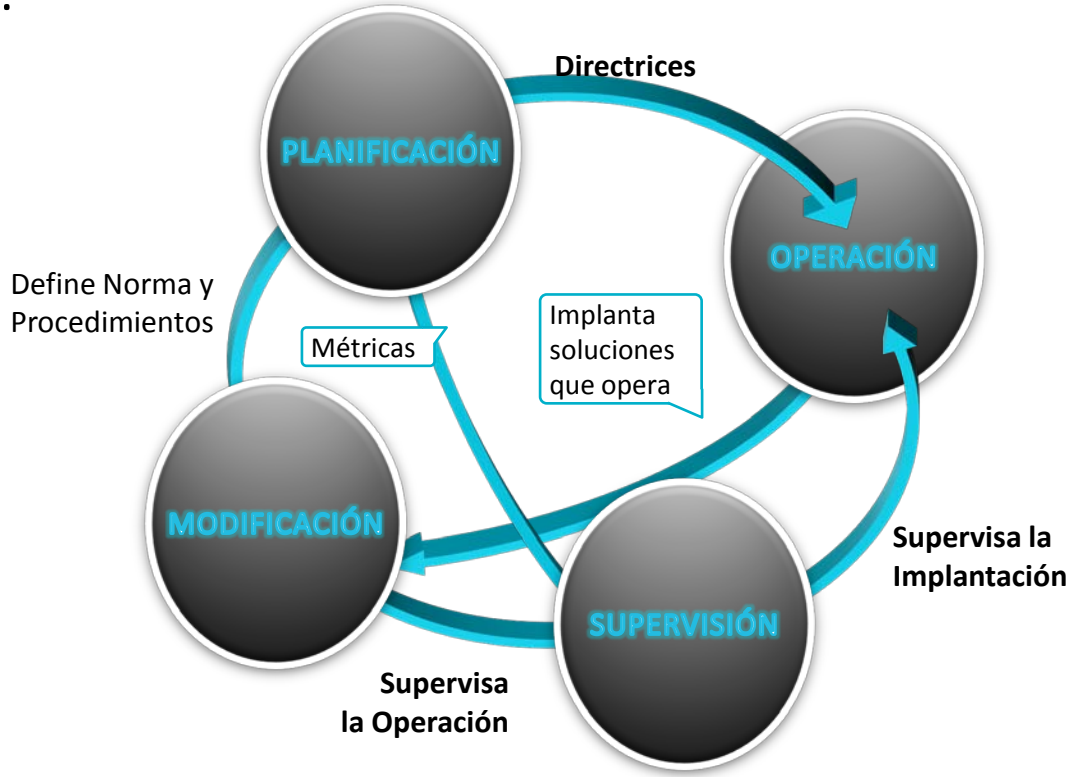
El adversario juega un papel activo, distorsionando la información e interfiriendo en las acciones a realizar

La información disponible requiere de un intenso y constante trabajo de refinamiento (eliminación de duplicidades, contradicciones, etc.)

LAS NUEVAS ESTRATEGIAS

LOS RETOS

- La seguridad como un proceso continuo totalmente integrado con el resto de procesos de las organizaciones.
- Capacidad para analizar, comprender y reaccionar
- Seguridad proactiva en tiempo real.
- Seguridad ligada al contexto.



CIBERSEGURIDAD Y CIBERDEFENSA

En Indra entendemos

CIBERSEGURIDAD

como el conjunto de tecnologías, procesos, procedimientos y servicios encaminados a proteger los activos (físicos, lógicos, o de servicios) de una empresa u organismo, que dependan en alguna medida de un soporte TIC

GRACIAS POR SU ATENCIÓN