CPITICM
Colegio Profesional de
Ingenieros Técnicos en Informática
de la Comunidad de Madrid

¿Se ha enterado que estamos en Ciberguerra?

Durante las últimas semanas de junio la mayoría de ciudadanos nos hemos enterado que nuestra sociedad, a la que denominamos "Sociedad de la Información", se encuentra en estado de ciberguerra.

Este documento pretende informar tanto a los ingenieros e ingenieros técnicos en informática como a la sociedad en su conjunto sobre la ciberguerra y exponer las consideraciones como profesionales de la ingeniería e ingeniería técnica en informática.

5 de Julio de 2013

Índice

¿Qué es la ciberguerra?

Durante las tres últimas semanas de junio la mayoría de ciudadanos nos hemos enterado de que nuestra sociedad, a la que denominamos "Sociedad de la Información"[1], se encuentra en estado de "Ciberguerra"[2 y 3]. La versión en español de la enciclopedia Wikipedia define como sinónimos "guerra informática"," guerra digital" y "ciberguerra", del inglés "cyberwar":

> *"Se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, en lugar de los campos de batalla convencionales.*
>
> *También se podría definir como el conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas del atacante. Los ataques informáticos no son considerados como ataques armados."*

Aunque la noticia le habrá inquietado se sentirá de momento algo más tranquilo, pues la ciberguerra tiene particularidades que la alejan mucho de las guerras tradicionales. Pero para la mayoría de los ciudadanos **aún será más desconocido que llevamos en estado de ciberguerra más de diez años** sobre los que especialistas, como el profesor Jorge Dávila[4] nos ofrece en su artículo "*Conclusiones de la Década de Ciberguerra*" que deberíamos tener en cuenta. Entre estas conclusiones llama la atención la que expresa de la siguiente forma:

> *"Además hay un problema aún mayor: **la militarización de la ciberseguridad**. Quizás el Pentágono con su apuesta por el quinto escenario[5] no esté militarizando el ciberespacio al propugnar robustas ciberdefensas, pero sí está **colaborando en militarizar las ideas y conceptos utilizados para analizar la seguridad en ese medio**. Está muy claro que los **ejércitos regulares deben prepararse concienzudamente para defenderse** de lo que, como a todos, nos puede pasar en el ciberespacio, pero no más. La misión física de los ejércitos reales no debe ponerse en riesgo por el hecho de querer utilizar el ciberespacio para su propio funcionamiento."*

Para muchas empresas, organizaciones públicas y privadas del planeta Tierra que durante las últimas semanas han tenido conocimiento de que el Ciberespacio, que todos conocemos como Internet, se encuentra en estado de ciberguerra, va a caer como un jarro de agua fría, pues gran parte de sus proyectos y estrategias actuales y

[1] http://es.wikipedia.org/wiki/Sociedad_de_la_informaci%C3%B3n
[2] http://es.wikipedia.org/wiki/Guerra_inform%C3%A1tica
[3] http://pt.wikipedia.org/wiki/Ciberguerra
[4] http://revistasic.es/index.php?option=com_content&view=article&id=855&Itemid=320
[5] Se consideran cinco escenarios bélicos: Tierra, Mar, Aire, Espacio exterior y Ciberespacio.

futuras están relacionadas con un mayor uso y aprovechamiento de las capacidades de Internet y de las nuevas arquitecturas informáticas basadas en la "nube"[6] o "cloud", para las que Internet es el soporte fundamental.

Muchos consejos de administración, gerencias, direcciones generales, etc., saber con pruebas objetivas e irrefutables que Internet está en estado de ciberguerra les ha de llevar en el corto y medio plazo a reconsiderar él "que", él "como", el "porqué", el "con quién", llevar a cabo el desarrollo de dichas estrategias en este escenario de Internet y del que desconocían que es considerado por grandes países un escenario bélico y en el que no habían considerado tan altos riesgos de seguridad, ni previsto mayores inversiones para mantenerlos bajo control.

¿Pruebas objetivas de que estamos en estado de ciberguerra

Si hace solo unos meses a un ingeniero en informática o a un abogado especialista en T.I., cualquier gran organización privada o pública le hubiera solicitado una asesoría con el fin de evaluar mejor los riesgo de seguridad en sus nuevas estrategias y proyectos basados en Internet y en la misma el profesional incluye recomendaciones basadas en que "*La ciberguerra es un futuro muy presente*"[7] es muy probable que le hubieran tomado por loco.

Todos, tanto a nivel personal como en las propias organizaciones públicas y privadas, estamos al corriente de los peligros de Internet y de las organizaciones criminales que utilizan la red como medio imprescindible para cometer sus delitos. No es objeto de este artículo entrar en detalle sobre el "malware"[8] (del inglés malicious software), ni de los medios más frecuentes utilizados por las organizaciones criminales, "Crimewar"[9] para perpetrar los delitos.

La palabra "ciberguerra" aún no ha sido registrada por el diccionario de la RAE, no obstante la palabra "guerra"[10] incluye múltiples acepciones y será muy sencillo ampliarla con la nueva acepción de ciberguerra. Es posible que la propia RAE sin, hasta ahora pruebas objetivas de que la ciberguerra es un hecho real, no ha decidido incluirla.

[6] http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube
[7] http://www.rtve.es/noticias/20130616/ciberguerra-futuro-muy-presente/689322.shtml
[8] http://es.wikipedia.org/wiki/Malware
[9] http://es.wikipedia.org/wiki/Crimeware
[10] http://lema.rae.es/drae/?val=guerra

No deja de ser llamativo que:

- el planeta ha tenido pruebas fehacientes de que estamos en ciberguerra precisamente porque una de las personas que hasta el pasado mes de mayo participaba activamente en la misma decidió "hacer la guerra por su cuenta"[11] para darla a conocer con el apoyo de poderosos medio de comunicación internacionales.
- **se nos achaca**, a la sociedad de la información en su conjunto, que **no habíamos entendido de que tras los atentados del 11 de septiembre de 2001 la guerra contra el terrorismo internacional también incluía, como parte fundamental la ciberguerra.**

Pero **hasta ahora desconocíamos como los principales países que los medios de comunicación citan como protagonistas: EE.UU, Rusia, Corea del Norte, Israel, etc. la estaban llevando a cabo**. Esto es lo que ha sido desvelado durante las últimas semanas del pasado mes de junio haciendo referencia a los medios concretos utilizados por EE.UU. En el anexo sobre "noticias de la ciberguerra" incluimos alguna de estas referencias para que cada cual saque sus propias conclusiones.

Si hemos de señalar que los hechos acaecidos son de extrema gravedad, como concisamente resume Heriberto Araujo en su artículo "Snowden apuntala la Ciberguerra mundial"[12] del pasado 1 de julio en que nos dice:

> *Lo que revela sobre todo el 'caso Snowden' son dos premisas que antes desconocíamos y que ahora deslegitiman a la Casa Blanca para liderar la lucha contra la anarquía en el ciberespacio.*
>
> - *Primero: Estados Unidos no espía sólo con el objeto de garantizar su seguridad nacional (¿qué hay de "estratégico para la seguridad nacional" en las sedes de la UE en Bruselas o Nueva York, o en la Universidad Tsinghua?), y por lo tanto podría haber espiado también con el objetivo de robar secretos industriales o información política.*
> - *Segundo: el sector "privado" (Microsoft, Facebook, Google, Amazon, Apple) y "público" en Estados Unidos no son completamente independientes el uno del otro, como aseguran, sino que se*

[11] El agente que sacude al espionaje mundial http://internacional.elpais.com/internacional/2013/06/28/actualidad/1372453017_337047.html

[12] http://blogs.elpais.com/conquista-china/2013/07/snowden-apuntala-la-ciberguerra-mundial.html

> *retroalimentan. No hablamos del mismo nivel que en China, donde los presidentes de las empresas públicas devienen de la noche a la mañana gobernadores provinciales, pero este caso refleja que la Casa Blanca aprovecha el tirón de Silicon Valley para espiar al planeta.*

Antes de conocerse estos hechos

> ***Estados Unidos era el único país** con la influencia suficiente para lograr que China –además de Rusia, Israel, Francia, entre otros- aceptara el establecimiento de normas consensuadas a nivel mundial **para deshacer el actual estado de ciberguerra, en el que cualquiera puede espiar con cualquier objetivo sin consecuencias, puesto que no existe un marco legal internacional que penalice al agresor.***

Es evidente que resultaría contradictorio para los Estados de Derecho del planeta que si con las Leyes que ya disponemos califiquemos de grandes organizaciones criminales, como la recientemente desmantelada red de de ciberespionaje NetTraveler[13] que ha afectado a más de 40 países y entre los 10 países más afectados se encuentra España, mientras que si hechos con bastantes similitudes son llevados a cabo por los servicios de inteligencia de países con Estados Derechos Democráticos **sean considerados legalmente inmunes bajo la etiqueta de "ciberguerra"**.

Los Estados de Derecho soberanos del planeta, las organizaciones de Estados plurinacionales como la UE que han asumido la Carta de Derechos Fundamentales[14], no pueden mantenerse como víctimas y espectadores de una "ciberguerra" que ellos no han declarado y que permite, con impunidad legal, violar los derechos fundamentales de sus ciudadanos.

También podemos observar como en este estado de ciberguerra y aprovechando los límites legales del derecho fundamental a privacidad e intimidad de la persona, ya hay organizaciones que no tienen mayores escrúpulos de violar las leyes que muchos países del mundo se han dado para protegerle y han visto un negocio a medio y largo plazo en la clasificación y elaboración de perfiles de personas en base a la captura de datos de las mismas sin su consentimiento: **para los jóvenes, o nativos digitales, estos hechos para ellos desconocidos podrían condicionar su vida futura**. Algunos detalles sobre este particular los resume muy bien Klint Finle, experto en Big Data, en su

13 http://www.cpiticm.es/w/documentos/publicos/Noticia%20seguridad%20informatica%207%20Junio%20de%202013.pdf

14 http://www.europarl.europa.eu/charter/pdf/text_es.pdf

artículo "*Deshumanización o fortaleza a través de los datos*" publicado el pasado 19 de junio. Sobre este particular la European Network and information Security Agency (ENISA)[15] publicó en 2008 un amplio informe denominado "*Desafíos inducidos por la tecnología en el ámbito de la intimidad y la protección de los datos en Europa*"[16], premonitorio de los hechos acaecidos. Se recomienda su lectura para entender mejor los hechos que se comentan en este documento.

Como consecuencia directa del conocimiento en el planeta de que nos encontramos en estado de ciberguerra ya están surgiendo los primeros conflictos diplomáticos por países que entienden que se está violando la legislación internacional que afecta a la soberanía de sus Estados de Derecho.

Dado que los hechos son recientes es difícil prever el impacto que tendrá en los ciudadanos y en las organizaciones públicas y privadas del planeta la necesaria confianza que se requiere para participar activamente en el desarrollo de la Sociedad de la Información. Lo que ha quedado claro es que la gravedad de los hechos marca un punto de inflexión y la necesidad de redefinir el camino que debemos seguir, camino que deberá estar basado en Leyes claras y bien conocidas por todos que sirvan de base a la necesaria seguridad y confianza.

Consideraciones desde la Ingeniería en Informática

1ª Condenamos los hechos acaecidos

La finalidad de la Ingeniería en Informática, como en el resto de Ingenierías, es "permitir que la Sociedad obtenga los mayores beneficios que la Ingeniería en Informática puede aportarla y evitar las amenazas y daños graves que dicha ingeniería puede ocasionarla". No se puede negar la importancia que para el desarrollo económico y social de todo país tiene el sector de la informática, además de los graves riesgos y peligros que para la vida de las personas, su salud, intimidad y la seguridad tanto individual como nacional suponen el desarrollo de actividades en este ámbito tecnológico.

Existe en la actualidad un alto grado de penetración de la informática en diferentes dimensiones de la Sociedad, tanto en aspectos más generales, como en otros que en particular tienen una incidencia directa en la intimidad, la salud, y la seguridad de las personas, así como en la propia Seguridad Nacional y las infraestructuras críticas. Es en este marco en el que el ingeniero en informática, como el profesional que

[15] http://www.enisa.europa.eu/

[16] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe-spanish-version

específicamente ha sido capacitado para el desarrollo de estas actividades con las garantías suficientes.

Condenamos los hechos acaecidos que han dado origen a la violación masiva de Derechos Fundamentales de ciudadanos europeos, en particular el derecho a la intimidad y privacidad el derecho a la protección de los datos de carácter personal, amparados por las constituciones, directivas y leyes de los países que integran la UE y manifestamos que dichos hechos se sitúan contra la Ingeniería en Informática y contra de las actividades profesionales de los Ingenieros e Ingenieros Técnicos en Informática.

2ª Exigencia de responsabilidades civiles y penales en el ámbito de la Informática

Los profesionales de la ingeniería e ingeniería técnica en informática contemplamos con la máxima preocupación como durante los últimos años se están produciendo hechos de gravedad, cuya raíz última se encuentra en la informática, sin que hasta la fecha dispongamos de un marco legal adecuado que permita la exigencia de responsabilidades:

- A las organizaciones, públicas o privadas, en cuyo seno se originan tales hechos,
- A los profesionales de la informática directamente relacionados con los mismos, ya sea como responsables del diseño, construcción y puesta en servicio de los sistemas informáticos cuyos fallos son la fuente o raíz de tales hechos, o como responsables de su adecuada utilización.
- A las empresas del sector de la informática que suministran los "componentes" físicos (hardware) y lógicos (software) con los que son construidos e integrados tales sistemas informáticos, y que en muchos casos son la causa del fallo.

3ª Compartimos las declaraciones y opiniones de la responsable de Justicia de la UE

Compartimos plenamente las declaraciones de la responsable de Justicia de la UE, Viviane Reding[17], al referirse a la gravedad de estos hechos poniendo de manifiesto que "***El concepto de seguridad nacional no significa que todo vale. Los Estados no tienen un derecho ilimitado de vigilancia secreta***".

> *"La gota que colma el vaso son esas informaciones que señalan que la Agencia Nacional de Seguridad estadounidense tiene acceso a los registros de llamadas de Verizon, At&T y Sprint, las mayores teleoperadoras norteamericanas, y que entre 2007 y 2011 las webs de Microsoft, Google, Yahoo!, Facebook, YouTube, Skype, AOL y Apple se integraron en un programa secreto que ha sido defendido por el presidente estadounidense, Barack Obama."*

[17] http://internacional.elpais.com/internacional/2013/06/12/actualidad/1371051599_670201.html

4ª Constatamos que los hechos se han realizado en un estado de ciberguerra secreta

Desde organizaciones profesionales de la ingeniería e ingeniería técnica en informática como ALI[18], y con la colaboración de la Universidad Politécnica de Madrid (UPM[19]) y de varios colegios de ingenieros e ingenieros técnicos en informática, así como de grandes compañías especializadas en seguridad y auditoría informática, durante los doce últimos años se están impartiendo cursos máster en seguridad y en auditoría informática. Dejamos constancia que durante tan largo periodo de tiempo en ningún momento hemos tenido conocimiento de los hechos comentados como consecuencia de la ciberguerra, hasta ahora secreta, que afectaba a la Sociedad de la Información. Y en ningún caso se consideraba que un Estado de Derecho podría representar graves riesgos de seguridad para terceros países: sus ciudadanos y sus organizaciones públicas y privadas.

5ª Gran impacto en la seguridad de los sistemas informáticos que prestan servicios en la sociedad de la información

Los hechos acaecidos obligarán a reconsiderar la seguridad en muchos de los sistemas informáticos que actualmente prestan servicios a través de Internet. Es muy probable que en los próximos meses tanto las organizaciones públicas y privadas deban revisar las medidas que están aplicando y también los aspectos de seguridad en contratos con terceros.

6ª Urgencia en cubrir los vacios legales relacionados con la Informática

Ponemos de manifiesto que probablemente los hechos comentados no alcanzarían tal gravedad si tanto en la UE, como en España no existieran los grandes vacios legales relacionados con la Informática en general e Internet en particular. Estos hechos deberán hacer reflexionar a la UE tanto sobre la necesidad urgente de superar tales vacios legales, así como la necesidad de propiciar unas mayores capacidades e independencia en tecnologías fundamentales para el desarrollo de la Sociedad de la Información en la UE.

7ª Colaboración sin reservas de los ingenieros e ingenieros técnicos en informática con las instituciones del Estado

Desde las asociaciones y colegios profesionales de ingenieros e ingenieros técnicos en informática nos ponemos a disposición de todas la Instituciones del Estado Español para contribuir con nuestros conocimientos y experiencia a solucionar las graves consecuencias de los hechos acaecidos.

[18] http://www.ali.es/
[19] http://www.upm.es/institucional

Anexo - Noticias de la ciberguerra

Se incluyen en este anexo las referencias a algunas de las noticias publicadas en las últimas semanas por el diario El País sobre el tema tratado.

Un joven experto en espionaje pone contra las cuerdas a Obama

La Unión Europea teme por la privacidad de sus datos

El secreto del revelador de secretos

Snowden denuncia el "amplio" ciberespionaje de EE UU a China

Europa inerme: Las autoridades europeas han facilitado que EE UU espíe de forma masiva a sus ciudadanos

Espionaje y libertades: La vigilancia masiva y secreta de las comunicaciones en EEUU socava la democracia

Las ventas de '1984' de Orwell se disparan tras la filtración de Snowden

La UE advierte a Estados Unidos de que la seguridad nacional no lo justifica todo

Obama defiende su programa de espionaje

EE UU solicitó a Facebook y Microsoft información privada de 50.000 clientes

EE UU dice que el programa de vigilancia evitó "docenas de atentados terroristas"

No quiero vivir en un mundo en el que se graba todo lo que digo y lo que hago

El Gran Hermano con la ayuda de Google

EE UU espió cerca de 500 millones de comunicaciones de Alemania

El agente que sacude al espionaje mundial

Hollande exige a EE UU que deje de espiar mientras Bruselas rebaja el tono

Snowden apuntala la Ciberguerra mundial