X JORNADAS STIC CCN-CERT

INTERVENCION DEL EMBAJADOR EN MISION ESPECIAL PARA LA CIBERSEGURIDAD – D. RICARDO MOR SOLA

Madrid, 14 de diciembre de 2016

Distinguidos participantes, señoras y señores:

Antes de nada quisiera agradecer al Centro Criptológico Nacional la oportunidad que me ofrece para que, en nombre del Ministerio de Asuntos Exteriores y de Cooperación, comparta con ustedes en esta sesión de clausura algunas reflexiones sobre la dimensión internacional de la ciberseguridad y presentarles una aproximación a las acciones coordinadas desde la Misión Especial que tengo el honor de representar, así como las acciones y tendencias observadas principalmente desde los organismos multilaterales en los que España participa y también en el ámbito bilateral.

Permítanme iniciar mi intervención con un enfoque que quizás a primera vista pueda resultar chocante: Internet, mientras perdure tal como lo conocemos hoy todos, se sostendrá en el tiempo sobre una arquitectura imperfecta. Y ello será así, a mi modo

de ver, porque Internet no surgió como una red de seguridad sino como una idea para la transmisión de información. Cuando se desarrollaron las primeras comunidades de internautas en los años noventa del siglo pasado se operaba sobre "redes" que muy raramente contemplaban esquemas de seguridad tal como los concebimos en la actualidad. La transición posterior a la "red de redes", esto es, Internet tal como ya lo vivimos en el siglo XXI, obvió la complejidad y la conflictividad de la naturaleza humana.

Aquel olvido, digámoslo así entre comillas, es lo que nos ha conducido irremediablemente al "parcheo" eterno de los sistemas operativos, componentes cibernéticos, dispositivos móviles, et cetera. Es cierto que ahora ya no hablamos de la seguridad de Internet, singularmente, sino de ciberseguridad, en la medida en que abordamos un espacio perfectamente delimitado –el ciberespacio- y que, tal como se acordó en la Cumbre de la OTAN en Varsovia, en julio pasado, ya es reconocido como un dominio de operaciones en el que la Alianza Atlántica "debe defenderse tan eficazmente como lo hace en el aire, en tierra y en el mar". Da vértigo, en efecto, la velocidad en que estamos inmersos a la hora de definir parámetros de seguridad que resuelvan las vulnerabilidades endémicas de Internet. Por eso, digo, mientras no surja una nueva arquitectura de la información y comunicación, distinta en su concepto y genética tecnológica, nuestra responsabilidad, hoy por hoy, ya sea desde los sectores públicos como desde los sectores privados, es tratar de seguir fortaleciendo la ciberseguridad a partir de las realidades presentes nacionales y en estrecha cooperación con nuestros socios, aliados y países amigos, algunos de los cuales – por cierto- han compartido con nosotros estas Jornadas a través de sus representantes diplomáticos acreditados en Madrid.

Amigos, no es únicamente una percepción personal de la cuestión lo que quiero hacer prevalecer en este discurso. Porque hay otra realidad que se ha constatado y se sigue constatando desde hace diez años como es el caso de estas Jornadas. Y es que, como todos los ponentes y participantes han demostrado en los debates y presentaciones de estos dos días, España cuenta con recursos tecnológicos y experiencia formidables en el ámbito de la ciberseguridad. También cuenta con un marco legal y normativo muy avanzado en comparación incluso con los países punteros en este ámbito en Europa. Es decir, contamos con herramientas avanzadas y en estos momentos estamos en fase de desarrollo de hasta nueve Planes Derivados del Plan Nacional de Ciberseguridad que abarcan los distintos aspectos referidos a la seguridad del ciberespacio.

Coincido plenamente con lo dicho por muchos de los ponentes que es necesario, en todo caso, fomentar aún más una cultura de la ciberseguridad, fundamentalmente entre los usuarios y responsables de los sistemas de información, tanto del sector privado y particulares como del sector público. Proporcionar seguridad a los sistemas de las Tecnologías de la información y Comunicación (TICs) es una tarea compleja, puesto que intervienen diversos elementos en la misma, difícil, pues en muchos casos la detección de los ciberataques es casi imposible, e incluso "ingrata", tal como el propio Secretario de estado Director del CNI, quien inauguró estas Jornadas en el día de ayer, ha escrito en el prólogo de una de las Guías del Centro Criptológico Nacional,

ya que -tal como él resaltó- “implica responsabilidades para la personas que tienen encomendada dicha seguridad”.

Señoras y señores:

Respecto a las realizaciones hechas por el Ministerio de Asuntos Exteriores y de Cooperación, y en particular a partir de los trabajos desarrollados por la Misión Especial para la Ciberseguridad que represento, permítanme resaltar brevemente algunos elementos que considero pueden ser de su interés en virtud de las oportunidades de expansión internacional que se pueden abrir o ampliar para los organismos, profesionales y empresas especializadas que han contribuido con sus experiencias respectivas en estas Jornadas.

España ha seguido participando a lo largo de 2016 muy activamente tanto en la UE como en los principales foros y organizaciones internacionales y multilaterales en los que la ciberseguridad se ha convertido en tema central, como Naciones Unidas, la OTAN, la Organización de Seguridad y Cooperación en Europa (OSCE), la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y el Consejo de Europa. España ha continuado defendiendo la necesidad de garantizar un ciberespacio abierto y seguro y la importancia de la cooperación internacional para lograrlo.

En el seno de Naciones Unidas, la participación de España como miembro No-Permanente del Consejo de Seguridad durante el período 2015-2016 ha tenido como efecto práctico en 2016 la organización de una reunión bajo el formato de Fórmula Arria el 28 de noviembre en la que, junto con otros expertos de los Estados Miembros, han participado los Miembros Permanentes y No Permanentes del Consejo de Seguridad. En dicha reunión se abordaron aspectos referidos al ciberespacio y su repercusión para la paz y seguridad internacionales, en particular en lo concerniente a la Protección de Infraestructuras Críticas basadas en las Tecnologías de la Información y Comunicación (TICs).

Cabe destacar que el Diario Oficial de la UE publicó el 19 de julio de 2016 la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (más conocida como “Directiva NIS”). Conforme a lo dispuesto en el artículo 26, esta Directiva entró en vigor para los Estados Miembros a los veinte días de su publicación en el Diario Oficial de la UE, esto es, el 9 de agosto de 2016.

Por otro lado, en 2016 se han ido desarrollando los ejes de acción sobre los que se articula el Plan Derivado del Plan Nacional de Ciberseguridad relativo a Cooperación Internacional y UE, aprobado en julio de 2015 y que coordina el Ministerio de Asuntos Exteriores y de Cooperación (MAEC). Dichos ejes de acción buscan potenciar la presencia de España en iniciativas relacionadas con la ciberseguridad, promover la armonización legislativa, la cooperación internacional, la participación en ejercicios y la construcción de capacidades, tanto en el ámbito operativo como en el institucional. En este sentido ha sido relevante la participación del Embajador en Misión Especial para

la Ciberseguridad en los diversos encuentros, conferencias y reuniones organizadas bajo los auspicios de UE, OTAN, OSCE, OCDE y Consejo de Europa.

En cuanto a la OSCE, España ha participado activamente en la preparación, negociación y adopción de la Decisión Nº 1202, de fecha 10 de marzo de 2016, adoptada por el Consejo Permanente de la OSCE en su reunión del 10 de marzo, relativa a Medidas de Fomento de la Confianza (MFCs) destinadas a reducir los riesgos de conflicto dimanantes del uso de Tecnologías de la Información y la Comunicación (TICs). Cabe recordar que, tras la aprobación en diciembre de 2013 del primer paquete de MFCs en materia de ciberseguridad, la OSCE encabezó la lista de organizaciones regionales que lograba consenso en materia de cooperación entre Estados en un aspecto de la seguridad internacional prioritario cooperación que ha sido reafirmada en el reciente Consejo Ministerial de OSCE celebrado en Hamburgo, Alemania, el 9 de diciembre.

Por otra parte, Naciones Unidas ha ido desarrollando una serie de recomendaciones a los Estados Miembros a través del Grupo de Expertos Gubernamentales (GEG) sobre los avances en el campo de la información y telecomunicaciones en el contexto de la seguridad internacional del que España ha formado parte durante el período 2014-2015.

Paralelamente, en el ámbito multilateral en 2016 ha tenido lugar en San José, Costa Rica, la Conferencia Anual de la Coalición para la Libertad en Línea (*Freedom Online Coalition,* FOC) el 17 y 18 de octubre, siendo ésta la primera vez en la que España participa como miembro de esta coalición gubernamental.

Se ha seguido con la aplicación de los diversos acuerdos bilaterales no normativos sobre cooperación en materia de ciberseguridad firmados el año pasado por España con la Organización de Estados Americanos (OEA), Marruecos, Paraguay y Perú, y se está a la espera de concluir otros Memorandos de Entendimiento bilaterales con diversos países del área iberoamericana en 2017, inspirados en el reciente Comunicado Especial sobre la Cooperación entre Autoridades Competentes en materia de Ciberseguridad suscrito durante la XXV (25) Cumbre Iberoamericana celebrada en octubre pasado en Cartagena de Indias, Colombia. Comunicado que, por cierto, fue promovido por España.

Asimismo, España ha participado en las actividades desarrolladas en 2016 por el *Foro Global para la Ciber Experiencia* (GFCE), cuya reunión anual, en la que por primera vez participó nuestro país como miembro de este foro, tuvo lugar en Washington del 1 de mayo al 2 de junio. España es, además, co-iniciador del proyecto GFCE sobre Protección de Infraestructuras Críticas de la Información (CIIP) y participante del proyecto GFCE-Organización de Estados Americanos (OEA).

Además, España ha participado en 2016 en la XII Conferencia del *Proceso Meridian* sobre Protección de Infraestructuras Críticas de la Información (CIIP), celebrada en México del 7 al 10 de noviembre, con contribuciones del CNPIC y el Ministerio que represento.

España también participa en las mesas redondas organizadas por el Consejo Europeo de Relaciones Exteriores (European Council on Foreign Relations). Dicha participación se corresponde con el compromiso adquirido por el MAEC en cuanto a la contribución de nuestro país a los debates desarrollados en diferentes foros multilaterales, incluidos los *think tanks*, en todas las cuestiones relacionadas con la seguridad del ciberespacio.

Por último, el Consejo de Ministros aprobó el 13 de mayo de 2016 la primera contribución a organizaciones no gubernamentales promovida por la Misión Especial para la Ciberseguridad, en esta ocasión en favor de ICT4Peace Foundation (Fundación TICs para la Paz), por un importe de 50.000 Euros, con cargo a los fondos que la Secretaría de Estado de Asuntos Exteriores tiene consignados para este fin en los Presupuestos Generales del Estado de 2016, bajo la siguiente rúbrica: ICT4Peace Foundation - Medidas para la lucha contra el uso terrorista de las Tecnologías de la Información y Comunicación (TICs). Aunque modesto, es un primer paso en lo relativo a la cooperación española internacional promovida desde el MAEC en el área de las Tecnologías de la Información y Comunicación (TICs) abordadas por la sociedad civil que, se espera, pueda incrementarse en próximos ejercicios presupuestarios. En el desarrollo del proyecto de ICT4Peace se han incluido tres talleres desarrollados durante el segundo semestre de 2016: Zúrich (25-16 de agosto), California (12-13 de septiembre) y Kuala Lumpur (18-19 de octubre).

A modo de conclusión, me gustaría trasladarles los siguientes comentarios:

Hay dos puntos que son de especial relevancia en el ámbito de las relaciones internacionales referidas a la ciberseguridad y respecto de los cuales España habrá de contribuir como socio europeo: por una parte, en el curso de 2017, está previsto que tanto el Consejo como la Comisión lleven a cabo conjuntamente una revisión de la Estrategia de Ciberseguridad de la UE de 2013 con el objeto de tener en cuenta los últimos acontecimientos en este área, y en aplicación de la Estrategia Global sobre Política Exterior y de Seguridad de la Unión; por otra parte, los ataques cibernéticos "presentan un claro desafío a la seguridad de la Alianza Atlántica y pueden ser tan perjudiciales para las sociedades modernas como un ataque convencional", esto es algo que ya subrayé al inicio de mi intervención.

Por último, amigos participantes, aun reconociendo que las dotaciones económicas tanto públicas como privadas se hacen cada vez más imprescindibles desde el punto de vista cualitativo y cuantitativo en todo lo concerniente a la ciberseguridad, aspecto éste en el que tanto gobernantes como particulares entendemos que hay mucho espacio para la mejora, no obstante también hay un sincero reconocimiento de que las capacidades de nuestros expertos, organismos especializados y posibilidades de expansión de nuestras empresas del sector en el extranjero para el desarrollo de capacidades de nuestros países amigos que lo requieran gozan de un nivel muy elevado y respetado. Y por ello me siento muy orgulloso de representar a todos ustedes en las relaciones diplomáticas de España en el exterior.

Parafraseando lo dicho por el Secretario de Estado en su intervención inaugural de estas Jornadas al referirse a la palabra "compañía", estoy seguro de que estarán de acuerdo conmigo en que para hacer frente a los desafíos que nos impone la seguridad del ciberespacio, en todas sus vertientes, ningún esfuerzo cabe escatimar, y para ello solamente la cooperación entre todos los actores interesados nos hará menos vulnerables, esto es, actores identificados en el sector privado industrial y pequeñas y medianas empresas, sociedad civil, mundo académico y universitario, y gobierno.

Pero, sin ánimo de competir en el deber que todos tenemos en este empeño de colaboración, se me ocurre referirme a lo que es tan nuestro como es El Quijote, precisamente cuando apenas faltan unos días para que termine este año 2016 en el que se conmemora el cuarto centenario de la muerte de Cervantes. Al respecto, les resumiré una historia que probablemente algunos de ustedes ya hayan escuchado en otros eventos. Hablando de "compañía", Ricardo Añino Vázquez, un compañero mío diplomático, hace ya un tiempo hizo un ingenioso símil que a modo de brindis final con ustedes me gustaría copiar y pegar.

Recordaba mi amigo tocayo que cuando en el capítulo 26 del libro primero, Don Quijote se decide por fin a comunicarse con su amada Dulcinea, tiene que pensar, además del contenido de su mensaje, el soporte que utilizará y el medio para enviarlo. Hoy en día -ya lo sabemos- los soportes y medios de comunicación son muy variados e instantáneos, pero Don Quijote tuvo que confiar sus pensamientos a una carta que entregó a su escudero Sancho para que la llevara a Dulcinea desde Sierra Morena a La Mancha. Lo primero que debe elegir es el soporte. No tiene papel, así que escribe la carta en un librillo de anotaciones. Esa es la primera decisión que toma todo comunicador: el soporte sobre el que grabar información, ya sea en un disco de un ordenador local o en un lejano servidor. Pero como el libro es pequeño y poco apropiado para una carta, Don Quijote le dice a Sancho que en cuanto llegue a un pueblo, le pida a algún maestro de escuela o a un clérigo, que la transcriban a papel. Esa labor del maestro es la que hoy en día realiza un nodo, que recibe información y la retransmite, o también un *interface*, que capta la información en un formato, aunque sea encriptado, y la transforma a otro más comprensible al ser humano.

Cuando mandamos un simple *sms* o un *whatsapp* desde nuestro móvil, podemos pensar que realizamos una acción sencilla, inmediata. Creemos que nos comunicamos directamente con otra persona, sin intermediarios, como si estuviésemos con nuestro interlocutor frente a frente. Eso nos da una falsa sensación de seguridad y confianza. Olvidamos por cuántas manos, por cuantas máquinas pasa nuestro mensaje hasta llegar a su destinatario.

Don Quijote encomienda la tarea a Sancho y éste hace un *back-up*. Por si pierde el librito, dice que recordará la carta de memoria. Es una estrategia imprescindible: no confiar la información valiosa a un solo soporte. Hoy día las empresas no confían sus datos sólo a sus ordenadores y servidores, sino también a eso que llamamos la nube. Uno se pregunta: ¿es segura la nube?

La “nube” de Don Quijote no era segura y el lector lo descubre unos capítulos más adelante. Sancho es interceptado en su camino por el cura y el barbero. Son amigos de Don Quijote, se preocupan por su salud, así que sonsacan a Sancho toda la información. El mensaje ha sido interceptado.

Sancho se da cuenta de que se ha olvidado el librillo en Sierra Morena, pero cuando echa mano de su memoria, ese segundo soporte de seguridad, queda patente que es bastante defectuosa. Al recitar de memoria la carta trastoca unas palabras por otras.

La historia continúa en el soberbio e ingenioso estilo de Cervantes, pero para acortar, decía mi compañero Ricardo, baste tan sólo decir que, cuando Sancho vuelve a encontrarse con su amo, se produce eso que es imprescindible en un entorno ciberseguro: la verificación por el usuario de que la información ha sido correctamente entregada. Don Quijote interroga a Sancho, se quiere asegurar de la fiabilidad de la comunicación. Pero Sancho hace lo que haría un peligroso *hacker*: tapa el rastro de su delito. Cuando Don Quijote le pregunta si entregó el mensaje y cómo lo recibió Dulcinea, Sancho inventa una sarta de mentiras que resume así el libro:

«La carta -dijo Sancho- no la leyó, porque dijo que no sabía leer ni escribir; antes la rasgó y la hizo menudas piezas, diciendo que no la quería dar a leer a nadie, porque no se supiesen en el lugar sus secretos, y que bastaba lo que yo le había dicho de palabra…».

He aquí algunas, amigos, si no todas, las enseñanzas de ciberseguridad escondidas en las páginas de El Quijote. Desde esta perspectiva literaria no parece que hayamos inventado mucho con Internet ¿cierto?

Enhorabuena a todos por el trabajo realizado en estas Jornadas y muchas gracias por su atención.