EL CIBERESPACIO, UN ASPECTO A TENER EN CUENTA EN EL PLANEAMIENTO MILITAR

CM (r) R. Mato Ex J.E.M. Cdo.de Ciberdefensa

El significado de la palabra planeamiento es “Elaboración o establecimiento de un plan”, y se denomina así al proceso metódico que se diseña con el objetivo de lograr una meta, es decir que el planeamiento es la elaboración de un plan que nos permitirá llegar a la concreción de un fin propuesto.

En las fuerzas armadas (FFAA) Argentinas actuales las tareas de planeamiento las realiza un organismo llamado “Estado Mayor”, en la cual para realizar el planeamiento se debe recopilar la información necesaria para redactar los planes y para asesorar al superior, como también para supervisar el cumplimiento de lo planificado.

Ahora bien, gran problema tendrán las FFAA en las que ni su estado mayor ni su jefe (al cual el estado mayor asesora), desconocen (pues no han investigado) cuál es la tecnología que dispone su oponente, o contra la cual se deberá planificar las operaciones.

Cuando un militar investiga respecto de las implicancias que las nuevas tecnologías (y en particular las tecnologías de la información y las Comunicaciones – TIC-) tienen en las operaciones militares podrá observar que la planificación de operaciones en el ciberespacio ya no es un tema que se aborda desde un punto de vista teórico (o escolástico) sino que ya hay FFAA que están realizando operaciones en el ciberespacio. Pero cuando vemos la realidad de nuestras FFAA, observamos que esta planificación sólo se discute en las escuelas de guerra, con lo cual llegamos a la triste conclusión que para muchos conductores y/o planificadores el ciberespacio sigue siendo un ámbito de conflictos para un futuro lejano.

Quizás el problema sea que quienes conducen las FFAA y la defensa nacional, y quienes tiene la responsabilidad de dirigir el planeamiento en sus diferentes niveles, todavía no conocen “bien” qué es el ciberespacio, en que se diferencia la ciberseguridad con la ciberdefensa / ciberguerra, que es un ciberdelito y cuál es la jurisdicción de cada uno de estos ámbitos; también desconocen porque es necesario que se redacte un diccionario en el cual se definan a nivel nacional cada uno de estos términos (y porque a nivel nacional, no solamente militar, pues ante la existencia de un evento en el ciberespacio que sea contrario a los intereses nacionales o de nuestra soberanía, la definición debe ser la misma para el poder político, para el militar, para el

funcionario de relaciones exteriores o para los profesionales en TIC o los del derecho).

El hecho que en nuestro país no se haya producido la evolución natural que ocurrió en el resto de los países del mundo (y en sus FFAA) respecto del paso del estadio de la “seguridad informática” hasta llegar al estadio de la “ciberdefensa/ciberguerra”, puede ser la clave de la situación actual, y de la falta de apoyo por parte de quienes dirigen las organizaciones de defensa (políticos y militares).

La evolución mencionada se dio al pasar de tener organizaciones basada en el papel y en medios analógicos a organizaciones que se fueron digitalizando de acuerdo con los desarrollos de cada época; a vuelo de pájaro describiré este cambio: así se paso del papel a las primeras computadoras, luego a las redes de computadoras, posteriormente a la interconectividad privada y finalmente a la interconectividad por Internet. Como ocurrió siempre en la historia humana, cada cambio llevó aparejado la implementación de diferentes medidas de seguridad, y así aparecieron la seguridad informática, la seguridad de la información y la ciberseguridad en el ámbito civil, y respecto del ámbito militar la evolución fue la inclusión de los sistemas informáticos como un medio de combate más (aparece la Guerra Informática como una parte de la Guerra de la Información) hasta llegar a la inclusión de un nuevo espacio donde se desarrollan nuevas operaciones: el ciberespacio y las operaciones en el ciberespacio.

Debe quedar muy claro que cada uno de estos hitos generaron cambios en la capacitación del personal, en los medios utilizados y en las operaciones a realizar, es decir que quién tenía la misión de planificar debía estar actualizado con esta evolución pues sino sus planes no servirían, un ejemplo para ilustrar el lector es el siguiente: si actualmente al planificar (sea el nivel que fuere) sólo se tiene en cuenta a las TIC como un servicio informático, y lo máximo que se ordena es que el área responsable implemente las medidas de seguridad o de contrainteligencia (es decir seguridad informática), ese plan y esa campaña, va camino al fracaso pues el oponente seguramente implementara operaciones utilizando el ciberespacio. Tener en cuenta lo siguiente:

- En la Cumbre de Varsovia que tuvo lugar entre los días 8 y 9 de julio de 2016, los jefes de Estado y de Gobierno adoptaron, entre otras, las siguiente medidas:

    1- Reconocimiento del ciberespacio como el quinto dominio de las operaciones militares.
    2- A través del documento Cyber Defence Pledge (NATO), se establece el compromiso por parte de los miembros de la Alianza en mejorar sus estructuras de ciberdefensa nacionales.

3- Declaración conjunta entre UE-OTAN para incrementar la cooperación en distintos ámbitos, entre ellos en materia de ciberseguridad y ciberdefensa. Posteriormente, en diciembre de ese mismo año, el Consejo de la UE aprobó cuarenta y dos medidas para desarrollar los acuerdos. (Documento 15283/16 del Consejo de la Unión Europea del 6 de diciembre de 2016).

- Durante la celebración del Foro Económico Mundial en enero de 2017 el secretario general de la OTAN, Jens Stoltenberg, afirmó que "los ciberataques pueden ser tan peligrosos y tan serios como un ataque armado, pueden dañar infraestructura crítica, causar daños a las vidas humanas y pueden minar nuestra capacidades de defensa ("can be as dangerous, as serious, as armed attacks. It can take out critical infrastructure, it can cause human injury and it can undermine our own defence capabilities"), volviendo a plantear la posibilidad de invocar el Artículo 5 de la Alianza.

Retomando la situación de la Ciberdefensa en nuestro país, que es lo que ocurrió respecto de la ciberdefensa?, pues lo mismo que ocurre en otros aspecto de la vida de nuestra nación: nos saltamos etapas y pasamos de un nivel básico (en este caso la "seguridad informática") a uno de los niveles más alto de la escala (la Ciberdefensa) sin experimentar las etapas intermedias, y lo que es peor, sin que quienes conducen estén convencidos acerca de lo que involucra ese salto.

Hasta el año 2014 nuestras FFAA apenas realizaban prácticas de seguridad informática y de seguridad de la información siguiendo estándares de la técnica que aplicaba el medio civil, y la sola implementación de estas medidas en las redes y sistemas administrativos costaba mucho trabajo a los responsables de seguridad en TIC, no se escuchaba los asesoramiento relacionados a que otros países desde el año 2006 ya incluían en sus misiones la defensa y el ataque del espacio ciber a través del uso de las redes digitales.

Del día a la noche, y a través de una norma administrativa, se pasa al nivel "Ciberdefensa" y se crea a nivel del Estado Mayor Conjunto de las FFAA (EMCFFAA) el Comando Conjunto de Ciberdefensa. En vez de "cambio por evolución" se dio un "cambio traumático" pues ni el EMCFFAA ni las mismas FFAA estaban maduras para ese cambio, mucho menos la dirigencia política.

El imponer un cambio a la fuerza trajo aparejado la falta de una estrategia de seguridad nacional en el ciberespacio, la falta de que exista un diccionario que haga que todos entiendan lo mismo cuando se cita un término (todavía se discute que es Ciberdefensa, cual es su alcance, diferencias entre la ciberseguridad y la Ciberdefensa, o creer que inteligencia en el ciberespacio es lo mismo que ciberinteligencia), no se ha definido que es un Ciberataque (pues una cosa es la definición técnica y otra la jurídica, y la jurídica tiene que verse desde el punto de vista del derecho interno y del derecho internacional público),

Este cambio por la fuerza trajo aparejado que todavía se estén discutiendo las responsabilidades de los organismos y de sus actores, desconociendo que en este nuevo espacio no hay fronteras como en el mundo físico o que uno de los tantos problemas que existe es asignar la autoría de un ataque (o delito) a sus autores.

Pero quizás, el peor de todos los problemas que trajo este cambio traumático fue la falta de capacitación de oficiales de comando para planificar operaciones en el ciberespacio y tratar cubrir esa deficiencia con personal cuyos conocimientos se limitaban a tareas de ciberseguridad, es decir la seguridad en el ciberespacio pero en el ámbito civil o de la empresa. En el medio civil la seguridad se limita, en general, a implementar medidas para evitar intrusiones o fuga de información, todo esto dentro de su perímetro (dentro de la empresa) y cuando ocurre un evento se denuncia y la justicia lo investiga. En el ámbito militar, además de implementar medidas de seguridad en las redes, se planifican operaciones de explotación (su objeto es obtener información de los sistemas del oponente, información del origen de ataques a sistemas propios), , defensivas (su objeto es mantener la libertad de acción) y las ofensivas (cuyo objeto es degradar, interrumpir, denegar o destruir sistemas de información del oponente o la información que los sistemas almacenan).

De todo lo detallado, vemos que producto de la falta de planeamiento se saltó de la seguridad informática a realizar operaciones en el ciberespacio sin la evolución correspondiente, y ese salto generó la mayoría de los problemas que se padecen actualmente. La situación es peligrosa pues se utiliza políticamente a la Ciberdefensa para los discursos pero no se solucionan los baches (gaps) existentes, quizás porque quienes dan esos discursos creen que el uso del ciberespacio para realizar operaciones militares es “ciencia ficción”.