Sebastián Beeche Ramírez

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	En el entendido que el manual de Tallin ya es conocido y manejado por quienes elaboran el reglamento, las respuestas y defensas frente a un ciberataque están cubiertas bajo ese ámbito, es importante recordar lo siguiente; Aunque se puede entender que la labor del estado es proteger y cuidar a la ciudadanía y no el proveerles telecomunicaciones, se debe entender que sin ellas, la misión del estado no puede ser completada, tal como sucedió en el ataque a Estonia el 2007 (y que dió origen al manual de Tallin por parte del grupo de Excelencia de la Otan). Para otorgar la "continuidad operacional" requerida, se debe primero establecer cuales son las infraestructuras críticas del país de cara a la ciudadanía (definidas en la PNCS), la primera es que quien tenga la RCE (Red de Conectividad del Estado) pueda mantener el servicio, mediante diversas tecnologías (F.O., pstn, móvil, satelital sobre centrales de comunicación u otros) y con diferentes niveles de prioridad de servicio, para que el estado mantenga comunicación hacia el interior de sus diferentes organismos a nivel central y luego a nivel regional y comunal con el ABC (Ambulancia (Hospitales), Bomberos y Carabineros) y los organismos civiles de mayor cuantía del lugar de forma de poder prestar la atención, al menos básica a toda la población que lo requiera. Si bien las infraestructuras de los operadores de telecomunicaciones son robustas desde la perspectiva de que están bien segmentadas entre redes

	administrativas (de usuarios) y de operación (antenas, routers, switches y servidores) sería deseable que dichas empresas y organismos realizar pruebas periódicas y estandarizadas de seguridad a las plataformas de acceso y control, frente a ataques externos y sabotajes internos que ponen en riesgo su continuidad operacional y que bajo una amenaza a la ciberseguridad, los protocolos de acceso no dependan de plataformas que puedan también verse afectadas y que generen un auto-baneo de los sistemas (como por ejemplo, utilizar Doble Factor de Autenticación en base a SMS para accesos a plataformas si éste también puede ser intervenido). Las infraestructuras críticas deben poder automantenerse en forma continua en caso de que sus suministros (energía principalmente) se vea afectada. Por otra parte, para las comunicaciones hacia el resto de proveedores críticos (banca, sistemas de alimentación, etc.) solicitar la utilización de sistemas de comunicación segura (VPN u otros) que permitan atenuación frente a ataques de Denegación de Servicio (DDoS) y que la información entre ellos no sea libre y abierta en internet, colocando barreras frente a la intervención de terceros. Se requiere mantener un canal de comunicación e información permanente hacia la población, por lo que tener una señal de radio y televisión con respaldo en los sistemas de transmisión (F.O, satelital, MM.OO., etc.) hacia las antenas de cada lugar se hace necesario.

	Por último, que bajo condiciones lo más cercanas a la realidad, y en forma periódica, se hagan las pruebas y simulacros globales correspondientes para que se generen las respuestas esperadas frente a dichos ataques y así observar y mejorar frente a este tipo de eventos, que de otra manera no pueden ser probados y de los cuales no se puede esperar que todo funcione a la perfección si lo que se prueba se hace sólo en laboratorio o con escenarios que no responden a la realidad de lo que podría suceder.