El mundo no está preparado para una CiberPandemia

Capitán de navío (Retirado) Germán Afanador Ceballos,
Armada de Colombia

Alertas sobre los efectos catastróficos que podría generar una pandemia venían siendo anunciadas hace años por conocedores y expertos en el tema. Bill Gates, entre varios, en el 2015, realizó una buena aproximación en una conferencia TED Talks.[1] Sin embargo, no fue mucha la atención y prioridad que estadistas y líderes prestaron en su momento a estos gritos de la comunidad científica, por lo que recursos, herramientas tecnológicas, análisis predictivos y personal capacitado no fueron orientados en hacerle un debido seguimiento al tema. No fue entonces sino hasta comienzos del año 2020, que se sintió el golpe devastador de su efecto a la salud pública, su propagación incontrolable y los daños nunca antes previstos a la economía, que se activaron tardíamente las alarmas—que desataron toda una serie de medidas reactivas en busca de estabilizar y amortiguar la estocada recibida.

Algo muy parecido o de escala superior podría presentarse en el corto plazo con los diferentes peligros que rondan en el ciberespacio. Las advertencias al respecto son muchas, desde hace tiempo. Existen diferentes centros de pensamiento reconocidos y programas bien estructurados auspiciados por grandes organizaciones, como la Organización de las Naciones Unidas (ONU), Organización de los Estados Americanos (OEA), Unión Europea (EU), entre otros, dedicados al tema. Sin embargo, es poco por parte de quienes están a cargo de tomar decisiones importantes los que han entendido de la amenaza, relegándola muchas veces como un problema que debe ser solucionado por los encargados de tecnología (IT por sus siglas en inglés) de instituciones, organismos y empresas. Estas alertas se han venido incrementando exponencialmente, teniendo en cuenta que la nueva normalidad con la que se está afrontando el COVID-19 está apresurando la transformación digital a un ritmo acelerado, cuyo fin es tratar de mantener a flote la economía, en medio del tsunami para el cual no se tenía un plan de mitigación contemplado.

Así las cosas, haciendo un paralelo con las enseñanzas que nos ha venido dejando el manejo de la pandemia, las amenazas del ciberespacio deben ser afrontadas de manera holística y transversal y no solamente por el encargado de tecnología o de seguridad. Así como contra el Coronavirus, los gobiernos, el sector productivo y la academia han unido esfuerzos en la toma de medidas preventivas

y búsqueda de soluciones integrales, de la misma manera se requieren acciones que permitan y faciliten de forma segura el buen uso del ciberespacio. Así como a través de fuertes campañas educativas las personas han logrado interiorizar que el autocuidado con el uso de mascarillas, lavado de manos y el distanciamiento social son fundamentales en la mitigación de enfermedades virulentas, se requiere que quienes se benefician de la informática entiendan que ese mismo autocuidado se asimila en el uso y cambio de claves frecuentemente, el no acceder a páginas inseguras, contar con antivirus y el empleo de *software* con licencia, entre otros, los cuales se convierten en normas mínimas básicas de ciberseguridad, que son efectivas en la mitigación del enemigo que acecha a todos desde el ciberespacio.

> Presidentes, Directores Ejecutivos (*Chief Executive Officers* – CEOs), militares y empresarios no han entendido que es responsabilidad de ellos la generación de estrategias de ciberseguridad que desciendan hacia todos niveles de sus equipos de trabajo y que su delegación en los encargados de seguridad y tecnologías los obliga a la constante supervisión de protocolos, procedimientos y mecanismos tendientes a brindar los niveles más altos de seguridad a sus empresas. Analizar constantemente el futuro en busca de riesgos es una decisión prudente y madura por parte de quienes tienen la responsabilidad de velar por la seguridad y trascendencia de sus compañías. ¿Qué está pasando?

Al tratar temas de ciberdefensa y ciberseguridad, existe una percepción generalizada y equivocada que solo compete a gobiernos y mega empresas que buscan proteger sus infraestructuras críticas, grandes activos e información sensible. La verdad es que son muchos los ejemplos de ciber ataques alrededor del mundo, como por ejemplo los de *Estonia* durante el 2007 y los de *NotPetya* y *WannaCry* en el 2017, los cuales dejaron en evidencia no solo los riesgos que presenta el uso del ciberespacio con brechas en temas de seguridad, sino las vulnerabilidades de Estados y multinacionales en la forma de cómo mitigarlos, afrontarlos y recuperarse de este tipo de incidentes. Haciendo una comparación, estos ciber ataques podrían asimilarse a las epidemias de la Gripe Aviar, Zika y del Ébola que en su momento levantaron banderas rojas de alerta de las cuales se creyó eran asuntos solo de países del tercer mundo, que debían ser abordados por científicos, médicos muy especializados y farmacéuticas multinacionales.

El COVID-19 ha tenido un impacto dramático en la población y ha forzado a que la sociedad, cada vez más, dependa de la informática y herramientas digitales que se soportan en la Internet. Lo que normalmente hubiese tomado años, hoy se está realizando en tan solo días y meses. La adopción a gran escala de tecnologías con acceso remoto que facilitan prácticas de trabajo desde la casa, con una mayor dependencia de los servicios en la nube (*cloud*) han permitido a las empresas continuar sus operaciones y reducir algunos costos; dando cumplimiento a las

órdenes de confinamiento decretadas por los gobiernos. Sin embargo, estas facilidades también están generando un incremento notable de riesgos provenientes del ciberespacio.[2] El Coronavirus ha forzado a que empresas y personas hayan pasado por una transformación digital apresurada en menos de cuatro meses convirtiendo el 2020, a la fuerza, en el año de la transformación digital.[3] No obstante, esta aceleración en el espacio virtual, de ensayo y error, está dejando vacíos de seguridad que están siendo aprovechados por ciber criminales, en especial si se tiene en cuenta que los recursos asignados para seguridad eran reducidos y que hoy en día algunos porcentajes de ellos se están destinando a atender la emergencia producida por la pandemia.

Esta pandemia nos ha enseñado cuáles son los verdaderos puntos críticos y sensibles de la sociedad. Lección que terroristas y criminales han asimilado con atenta nota para su aprovechamiento. Según reportes de la ONU, desde la emergencia de la pandemia cada 39 segundos existen evidencias de ataques cibernéticos a nivel global. De igual forma se han incrementado en un 600 por ciento correos maliciosos, así como se han venido perpetrando ciber ataques consecutivos contra organizaciones de salud.[4] Otro informe del *Cyber Threat Intelligence League* indica que los *hackers* están atacando todos los estamentos, tratando de robar toda la información posible no solo la relacionada con el Coronavirus.[5] Según el informe *Managing the Impact of COVID-19 on Cyber Security* desde el pasado mes de enero, cuando la pandemia estaba en su fase inicial, temas relacionados con el COVID-19 fueron empleados de forma masiva para diseminar, a través del ciberespacio, troyanos y *software* infectados con el fin de penetrar los sistemas informáticos de las empresas.[6] El centro médico de Parkview en Colorado, EE.UU., fue víctima de una ciber intrusión a sus sistemas de IT que lo forzó a depender de historias clínicas en papel, en pleno tratamiento de pacientes con Coronavirus.[7] De igual manera, algunas naciones están aprovechando el COVID-19, para a través de ciber inteligencia, infiltrarse en los sistemas gubernamentales y corporativos de otros Estados y realizar espionaje.[8] Recientemente, diferentes sectores, tanto públicos como privados, en Australia fueron víctimas de sofisticados hostigamientos a través del ciberespacio, presuntamente provenientes de un estado hostil.[9] Ciber ataques que como la curva de la pandemia se han venido propagando de manera exponencial y parecen no encontrar pico para empezar a aplanarse, por lo que se podría afirmar que un ciber ataque con características similares a las del Coronavirus se lograría propagar más rápido y tener una mayor cobertura que cualquier virus biológico.[10]

¿Cuál es el camino a seguir?

El COVID-19 cambió por completo el estilo de vida de la población mundial, disparó las medidas biosanitarias, así como nuevas normas y regulaciones. Es evidente que enfrentar esta amenaza ha requerido un esfuerzo conjunto por lo que se recomienda a las instituciones, organizaciones y empresas actualizar sus procedimientos de trabajo remoto mientras verifican y refuerzan sus políticas de seguridad informática debido a que la resiliencia cibernética de las empresas requiere de un esfuerzo multidisciplinario combinado y alineado en busca de una cohesión empresarial y aprovechamiento de todas las oportunidades digitales.

Gobernantes, militares de alto rango, CEOs y empresarios deben tener en cuenta que definir y modelar el universo de amenazas que pueden afectar su organización es de su entera responsabilidad. En lo que al ciberespacio se refiere, para empezar, se requiere contar con la capacidad de detectar cuando un adversario ya tiene infectados los sistemas propios. En casos demostrados se ha podido establecer que ciber espías han podido permanecer ocultos, por largos periodos de tiempo, dentro de los sistemas informáticos de las empresas sin ser detectados, inclusive aun después de haberse realizado inspecciones internas de ciberseguridad.[11] Terminar en una unidad de cuidados intensivos informáticos es demoledor para una organización, por lo que el tratamiento para reponerse es contar con un equipo experto (intensivistas) y actuar con la mayor rapidez. Estar preparados, parece ser la mejor estrategia para sostener la economía de los países en la inminente ciber pandemia.

Paralelamente, como en la pandemia, se requiere proteger los grupos de riesgo adoptando aproximaciones de ciberseguridad proactivas que permitan, de manera efectiva, identificar las vulnerabilidades en los sistemas, antes de que se vean comprometidos. Esto solo se logra realizando un amplio monitoreo de las redes, practicando el *hackeo* ético, capacitando constantemente a todo el personal y realizando auditorias de ciberseguridad por intermedio de expertos completamente independientes a la organización.[12]

En la elaboración de los planes de mitigación de riesgos, se debe tener claro que la ciberseguridad es transversal a todos los procesos de la empresa. La ciberseguridad por si sola en una organización se queda coja. Es imprescindible que todo trabajador, independientemente de su nivel en la empresa, que acceda a un computador, una tableta o un teléfono inteligente, debe entender que procesar datos y archivos, a través de medios informáticos, los vuelve potencialmente susceptibles a ser saboteados, robados y espiados—por lo que debe contar con el debido entrenamiento y supervisión para evitar este tipo de incidentes. De lo contrario, existe un alto riesgo de poner en peligro el capital informático, prestigio e información

clasificada de la organización o empresa para la que labora. Por lo que es de suma importancia contar con talento humano calificado y realizar constantemente campañas educativas en todos los niveles de la organización.

Conclusiónes

Si algo ha permitido que durante esta pandemia las infraestructuras críticas y la economía se hayan podido mantener en medio del huracán, es la Internet, la virtualidad y el trabajo remoto. El no tomar las medidas preventivas, con la suficiente anticipación, en cuanto a la regulación y buen uso del ciberespacio, podría desencadenar en un brote cibernético que llevaría a la sociedad a sumirse en una ciber cuarentena prolongada, mientras se recuperan datos, archivos, programas y se corrigen los sistemas infectados, alterados o bloqueados. Situación está que sería muy seguramente más catastrófica a la que vivimos en la actualidad. ❑

Notas

1. Bill Gates. ¿La próxima epidemia? No estamos listos. https://www.ted.com/talks/bill_gates_the_next_outbreak_we_re_not_ready?language=es.
2. Cybersecurity Leadership Principles. Lessons Learnd During the COVID 19 Pandemic to Prepare for the New Normal. World Economic Forum. May 2020.
3. Enrique Dans. La Crisis del Coronavirus y el Darwinismo Digital. https://www.enriquedans.com/2020/04/la-crisis-del-coronavirus-y-el-darwinismo-digital.html.
4. Izumi Nakamitzu. Alta Representante de la ONU para asuntos de Desarme. https://forbes.co/2020/05/22/actualidad/se-calcula-que-hay-un-ataque-informatico-en-el-mundo-cada-39-segundos-onu/.
5. They are trying to steal everything. US Coronavirus response hit by foreign hackers. https://edition.cnn.com/2020/04/25/politics/us-china-cyberattacks-coronavirus-research/index.html
6. Managing the Impact of Covid-19 on Cyber Security. Marzo 2020. https://www.pwc.es/es/covid-19/ciberseguridad-gestionar-impacto-covid19.html.
7. Bulletin on recent ransomware and disruptive attacks. The Chertoff Group. Junio 2020
8. Cybercrime, Threats Turing the COVID 19 pandemic. Global Initiative against transnacional organizad crime. Abril 2020, pag 10
9. The Guardian. Cyber Attack Australia: Sophisticated attacks from state based actor. https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison.
10. What Covid 19 Pandemic teaches us about cybersecurity. World Economic Forum. https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/.

11. El colombiano que vendió una multinacional de ciberseguridad y creo una nueva que esta volando. Revista Forbes. https://forbes.co/2020/07/06/emprendedores/ricardo-villadiego-vigilante-de-la-red/.

12. Proactive Vs Reactive Cybersecurity. Experts opinions. https://www.vpnranks.com/blog/proactive-vs-reactive-cybersecurity-expert-opinions/.

Capitán de Navío (Retirado) Germán Afanador Ceballos, Armada de Colombia

Consultor empresarial, conferencista, basta experiencia en temas de ciberseguridad, análisis de Riesgos y Planeación estratégica con 30 años de experiencia. Estudios en Colombia y el exterior relacionados con Ingeniería Naval Electrónica, Ciencias Navales, posgrados en Seguridad, Defensa Nacional, Estudios Políticos y Maestría en Estudios Estratégicos de Seguridad.

Su experiencia está enmarcada en la implementación de planes de seguridad y continuidad del negocio para protección de activos y desarrollo de funciones críticas; gestión de estudios, auditorias de seguridad e información y convenios con agencias locales e internacionales orientados a fortalecer capacidades corporativas; Asesoría a Juntas Directivas de la empresa privada, en temas estratégicos y de seguridad. Destacado liderazgo y orientación de grupos grandes personas hacia el logro de objetivos estratégicos.