Editorial

La evolución de la tecnología de la informática ha producido significativos adelantos y beneficios para la humanidad, al mismo tiempo que ha creado serios problemas relacionados con el alarmante auge de la delincuencia cibernética, el ciberespionaje, los ataques cibernéticos, y la inminente amenaza de una guerra cibernética. Y no se trata de algo que pueda suceder –es algo que ya se está librando. La difusión de la tecnología digital y las consecuencias de un inesperado ataque cibernético de mayores consecuencias ponen en peligro el orden y la seguridad mundial. Algunos advierten que los efectos de una guerra cibernética pueden ser tan destructivos como los de una guerra nuclear. De acuerdo con el presidente de la Comisión de Comercio del Senado, Jay Rockefeller, *"Los criminales cibernéticos de hoy en día tienen la capacidad de interrumpir los servicios de mantenimiento de la vida, causar catastróficos daños económicos, o degradar severamente las redes de las cuales depende nuestra defensa nacional y nuestras agencias de inteligencia."* Coherente con esta misma línea del pensamiento, encontramos el pronunciamiento bien fundamentado del Secretario de Defensa de los Estados Unidos y ex director de la CIA, León Panetta: *"Lo cierto es que existe la capacidad cibernética para tumbar nuestras redes eléctricas y/o paralizar el sistema financiero de nuestro país. Por lo tanto, considero que tenemos que estar preparados no solo para defendernos contra esta clase de ataques sino también, en caso necesario, para ser agresivos"*. Los Estados Unidos y muchos otros países se muestran actualmente vulnerables frente a la posibilidad de un ataque catastrófico inesperado, equivalente al de Pearl Harbor, del cual podrían ser víctimas inequívocas. Por lo tanto, no se pueden descuidar ni dejar de reforzar sus defensas cibernéticas como parte de su estrategia militar. Conscientes de esta realidad y de la seriedad que conlleva esta amenaza, dedicamos esta edición al tema de la guerra cibernética.

Teniendo en cuenta lo anterior, podemos afirmar que el entrenamiento y la preparación de nuestros líderes militares constituyen la forma mas acertada para enfrentar la amenaza de una guerra cibernética. Siendo consecuente con esta necesidad, el Teniente General Fadok y el Dr. Raines nos ofrecen su visión sobre la guerra cibernética en el artículo titulado "Encaminándonos hacia el éxito en la misión cibernética de la Fuerza Aérea" y presentan además los programas existentes y los planes futuros de la Universidad del Aire, respecto a la preparación académica de nuestros líderes para luchar exitosamente en futuros conflictos que abarquen todos los ámbitos posibles, tales como: agua, tierra, cielo, espacio, y ahora el ciberespacio.

Por otro lado, no podemos omitir las consideraciones más difíciles que enfrentan nuestros líderes, tanto civiles como militares, y que se originan en las diferencias ideológicas entre la ética y la ley relacionadas con la cibernética aplicada a las operaciones, ya que éstas pueden causar destrucción masiva por estar regidas por leyes internacionales de la guerra –aunque aún no muy claras en relación con la guerra cibernética. En su ensayo titulado "La intersección de la ley y la ética en la ciberguerra" el General Dunlap puntualiza algunos temas que ilustran cómo los conceptos legales y éticos se cruzan en el ámbito del ciberespacio, y concluye que los actuales principios básicos de la ley de los conflictos armados son suficientes para hacer frente a los temas más importantes de la guerra cibernética.

La propagación del gusano cibernético conocido como *Stuxnet* marca el primer episodio de una nueva era en los anales de la guerra moderna, similar al primer uso de armas nucleares. Su difusión debe hacernos tomar conciencia sobre la necesidad de una adecuada preparación que impida que las naciones se enfrenten a una guerra en el ciberespacio sin antes despejar muchos interrogantes relacionados con la ciberseguridad y las leyes cibernéticas. Stuxnet, el arma cibernética más sofisticada del mundo hasta el momento, fue un programa de sabotaje masivo de secreto a alto nivel dirigido a las instalaciones de enriquecimiento de uranio de la planta Natanz, Irán, en donde se destruyeron alrededor de 1000 de las 5000 centrífugas iraníes y con el que frenaron el programa nuclear de Irán. El gusano Stuxnex fue increíblemente complicado y sofisticado como lo detalla mucho mejor el Mayor Shakarian en su artículo "Stuxnet: Revolución de ciberguerra en los asuntos militares."

Los ataques contra los sistemas de información e infraestructura tanto del gobierno como de las organizaciones privadas y gobiernos extranjeros, podrían derivarse en un futuro no muy lejano, en un conflicto militar a gran escala. El peligro más grande de un ataque cibernético proviene de la ca-

rencia de un mecanismo internacional de regulación de las armas cibernéticas, incrementado por la dificultad de determinar con seguridad y exactitud el origen o intento de un ataque y la posibilidad de que un país erróneamente pueda actuar en contra de otro país que no hubiera tenido participación directa o indirecta en el ataque. El Dr. Crosston sostiene en su escrito "El mundo se ha vuelto "ciberloco", que una política de disuasión equilibrada y clara sería mucho más efectiva y deseable que una política solo de disuasión defensiva. Crosston concluye, que frente a una doctrina de destrucción cibernética mutuamente asegurada, basada en un temor mutuamente compartido de una amenaza ofensiva, los adversarios perderían el incentivo de iniciar un ataque.

Para un mayor entendimiento acerca de los aspectos concernientes a la evolución, retos, y lecciones aprendidas del Poderío Aéreo y los que actualmente presenta el nuevo ámbito ciberespacial, es necesario que repasemos la historia del viejo y nuevo ámbito. Al respecto, el Teniente Lee en su artículo titulado "Los años interinos del ciberespacio" analiza las ventajas, similitudes y diferencias del poder de la cibernética y se pronuncia sobre los ataques cibernéticos más recientes, concluyendo que para poder tener éxito en el ámbito ciberespacial, el DoD y los socios civiles deben hacer mayor énfasis en la educación y el entrenamiento de la próxima generación de líderes cibernéticos.

Para ilustración de todos en esta materia, es conveniente tener en cuenta que este año se ha realizado un número sin precedentes de eventos catalogados bajo el tema de la guerra cibernética. Nuestra base industrial ha sido el objetivo de muchos de estos "ciberataques" mostrándose vulnerable a los ataques de espionaje o de robo de propiedad intelectual por parte de gobiernos y delincuentes cibernéticos. Pese al esfuerzo continuado de la política de ciberseguridad de Estados Unidos para responder a estos desafíos, encontramos aún intervalos críticos y vitales para la seguridad industrial y nacional. En su escrito titulado "Preparación de la inteligencia del entorno de información y comunicaciones" el Sr. Carr propone una función que ha llamado Preparación de Inteligencia del Entorno de Información y Comunicaciones (IPICE), cuya implementación mejoraría la táctica defensiva, por parte de entidades tanto comerciales como gubernamentales.

Continuado la reflexión en esa misma dirección Chang y Granger, autores de "La Guerra en el Ámbito Cibernético", aciertan cuando afirman que para diseñar exitosamente una estrategia en el nuevo campo de batalla, es necesario comprender y asimilar el nuevo concepto cibernético, sin descuidar nuestras vulnerabilidades cibernéticas, facilitando para ello el intercambio de información y los mecanismos de coordinación de la seguridad e involucrando en la educación a todos los actores militares y civiles.

Finalmente, agotamos la cobertura del ciberespacio y la guerra cibernética con la presentación de dos interesantes artículos escritos uno por el Teniente Coronel (Ret) Jeffey Hukill y el otro por el Capitán John Cobb. De acuerdo a su presentación, Coob en su artículo "Virtualmente masivo: comprendiendo la concentración y el poder de combate en la ciberguerra", hace un paralelismo entre el concepto del efecto de un ataque masivo cibernético sumamente preciso y concentrado, lanzado por medio de un gran número de paquetes de bitios o de un gran número de viruses liberados simultáneamente y el efecto de varios ataques devastadores lanzados desde cualquier parte del mundo, por un puñado de agresores. A su vez Hukill, en su escrito titulado "Pautas para diseñar estructuras adaptativas de mando y control (C2) para las Operaciones Ciberespaciales", basado en un estudio sobre el C2 ordenado por el General Mark Welch, Jefe del Estado Mayor de la Fuerza Aérea, y en que él fue un participante, sostiene que el enfoque en operaciones ciberespaciales exige un C2 adaptable apoyado en la descentralización de decisiones, intercambio de información e interacción entre comandantes y planas mayores al nivel de organización más bajo capaz de integrar recursos.

Teniente Coronel Luis F. Fuentes, USAF-Retirado
Editor, *Air & Space Power Journal—Español*