HIC SVNT LEONES.[1]

La seguridad informática y de telecomunicaciones de un Estado.

Grl Div (R) Evergisto de Vergara[2]

"Me dan diez piratas informáticos cuidadosamente escogidos,
y en los próximos 90 días, sería capaz que esta nación
deponga sus armas y se rinda."
J. Saiteerdou, Delitos Informáticos del FBI[3]

Tradicionalmente, los ámbitos o dominios donde se desempeñaba el componente militar del poder del Estado eran tres: aire, mar y tierra. A mediados del siglo pasado, con la aparición de los satélites y su uso militar, se agregó un ámbito más: el del espacio. A fines del siglo pasado, con la aparición de nuevas tecnologías de información, surgió el espacio cibernético. Ninguno de los dos últimos ámbitos reconoce fronteras geográficas ni políticas.

La tecnología ha avanzado a pasos tan agigantados, que se ha creado una brecha generacional. Personas de más de 50 años no entienden que ocurran cosas que antes se reservaban para libros de ciencia ficción. No solo eso: la tecnología avanza a pasos tan desmesurados, que va por delante de la capacidad del hombre para aprehenderlos. Para graficarlo, la tecnología de información pasó de válvulas de la década del 50 (las radios RCA Victor), a los transistores de la década del 60 (la conocida y revolucionaria en ese entonces radio

[1] Expresión usada en la antigua Roma, para indicar un terreno inexplorado peligroso.
[2] El autor agradece la colaboración del Capitán de Navío Eduardo Traina en la elaboración de este artículo.
[3] Citado en Qiao Liang y Wang Xiangsui, Unrestricted Warfare, Pan American Publishing Company, Panama, 2002, P. 112.

Spika), y a los chips y microchips de la década del 80 (los procesadores de computación). Es inútil adquirir la última tecnología, que pasará a ser vieja en pocos años. Se crean entonces brechas culturales, que los de más edad ya la sufren, cuando prefieren conservar su viejo teléfono móvil antes que aprender a manejar uno de última generación.

Aquellos que conocieron las primeras computadoras en EEUU a mediados de la década del 60, en las cuales la información se introducía en tarjetas perforadas, también conocieron las primeras computadoras personales Commodore, las PC XT con disquetera 5 ¼ y una enorme entonces capacidad de disco de almacenaje de hoy insignificantes 10 MB en 1985, y las actuales con CD, 200 o más GigaBytes y procesadores veloces, que muy pronto dejarán de serlo y serán reemplazados por otros mas eficientes. Nadie se da cuenta hoy que, en 1995, la hoy difundida *banda ancha* de internet no existía ni en EEUU. La fibra óptica como medio de trasmisión se difundió recién en 1988: a partir de allí se podía trasmitir una gran cantidad de información a grandes distancias. Ya están en camino los nanoprocesadores.

Todo este progreso sinérgico nació cuando el ser humano descubrió que podía grabar información en el elemento más abundante sobre la tierra: el silicio, comúnmente denominado arena. Se sumó esta capacidad de almacenar información, con la necesidad de trasmitirla velozmente, y procesarla cada vez más rápidamente. Su primera consecuencia práctica fue la Internet, un modo de interconectar redes de computadoras compuestas por millones de artefactos de computación.

El origen de Internet fue militar: en plena Guerra Fría y ante la amenaza del holocausto nuclear, había que inventar un sistema por el cual si Washington o Moscú eran destruidas por bombas nucleares, las comunicaciones no fueran interrumpidas. Para eso se pensó en todas las líneas telefónicas dispersas en el mundo. Esas no podían ser destruidas. Surgió así en 1962 ARPANET [4] en el ámbito de la Defensa en EEUU.

En ese entonces nadie notó que la información daba poder, y que requería de cierta confidencialidad: nadie pensó en privacidad, protección de datos, integridad de datos,

[4] ARPA es la abreviatura de Advance Research Proyect Agency, la agencia de defensa de USA que lo diseñó. net significa "red".

disponibilidad, consistencia, control de las redes, auditoría der redes. Internet permitía la transferencia de datos, y la muy conocida www (world wide web) es solo uno de los servicios que proporciona internet. Además, internet incluye correo electrónico, transferencia de archivos, control remoto de computadoras, y otros servicios.

El espacio cibernético

Se creó así un nuevo espacio: el denominado *espacio cibernético* que es un ambiente dentro del cual interactúan muchos participantes con capacidad de influirse mutuamente, e incluye *una red interdependiente de infraestructura de tecnología de la información que incluye la internet, redes de telecomunicaciones, sistemas de computación, y procesadores y controladores dedicados a tareas de procesamiento de datos en tiempo real.* [5]

Lo que parecía ser un avance en el desarrollo del género humano, pronto fue desviado para otros propósitos no tan loables. El uso de la tecnología informática invadió con velocidad todos los campos del quehacer humano, y su dominio se extendió al alcance de todos, sin necesidad de grandes recursos. El primer mal uso de la informática que surgió fue el delito común: el primer caso de robo informático que se tiene conocimiento ocurrió en Estados Unidos: un empleado de un banco que usaba esta nueva tecnología, al darse cuenta que las transferencias bancarias quedaban asentadas en un disco rígido y su primer pista era borrada diariamente para permitir el ingreso de datos nuevos, se transfirió varios millones de dólares a una cuenta que había abierto en Suiza, y luego grabó la operación en la primer pista del disco duro. Al día siguiente, al banco le faltaban esos dólares, y no quedaban rastros de la transferencia. Finalmente este ladrón informático fue apresado, cuando con el dinero de la operación fraudulenta fue a comprar diamantes a Arabia Saudita, y no como producto de la detección de la forma de fraude cometido. Es un principio que aplican las fuerzas policiales del mundo, que dice que por naturaleza humana, la ansiedad con la que un ladrón roba es la misma que tiene para gastar el dinero robado.

Apareció entonces una nueva raza, los denominados *hackers*, usuarios con conocimientos para encontrar vulnerabilidades en redes de computación. Existen *hackers* de todos los tipos y

[5] No existe todavía una única definición internacional consensuada.

colores: los hay inofensivos y delictivos, aislados o en equipo. En 1994, un hacker en Inglaterra atacó el *US Military Rome Air Development Center* en el estado de Nueva York, comprometiendo la seguridad de 30 sistemas; También había atacado otros 100 sistemas. El *Korea Atomic Energy Research Institute* (KAERI) y la NASA sufrieron daños, entre otros. La gente quedó atónita no solo por la escala del daño, sino también por el hecho que el hacker tenía solo 16 años. En 1994, hubo 230.000 intrusiones relacionadas con la seguridad en las redes del Departamento de Defensa de los Estados Unidos. ¿Cuántas de ellas fueron actos destructivos organizados por guerreros no profesionales? Tal vez nunca habrá forma de saberlo. Todos los tipos de los piratas, con diversos fondos y valores, se esconden bajo redes de camuflaje: estudiantes de secundaria curiosos; buceadores *on line*; miembros de un personal de asesoramiento que guardan rencores o envidias; una red recalcitrante de terroristas; Estados en busca de poder; y mercenarios de la red. En sus ideas y en sus acciones, este tipo de personas son polos separados, pero que se agrupan juntos en el mismo mundo de la red. Ven su ocupación conforme a sus propios juicios de valor distintivos y sus propias ideas que para ellos tienen sentido, si bien algunos están simplemente confundidos y sin rumbo. Por estas razones, si están haciendo bien o haciendo mal, no se sienten obligados por las reglas del juego que prevalecen en la sociedad en general. Usando computadoras, podrán recabar información por las buenas o por las malas de las cuentas de otras personas. Pueden eliminar valiosos datos de otra persona, que se obtuvieron con tantas dificultades, como una broma. O, como el legendario caballero errante solitario, pueden usar sus conocimientos técnicos en una línea tendiente a asumir el poder del mal. [6] Esta nueva guerra sin enfrentamientos militares, anónima fuera de todo ámbito legal, norma ética o límite, ya había sido anticipada en el libro *Unrestricted Warfare* escrito en Diciembre de 1999.[7]

La falta de seguridad en los sistemas del espacio cibernético comenzó a asolar el campo militar. En 1996, el Jefe de Inteligencia del Pentágono alertó sobre un joven argentino de 18 años desde Buenos Aires, había penetrado vía Londres los archivos secretos de esta estructura militar estadounidense. Casi de manera homóloga al caso anterior, este joven fue detectado porque había alardeado y hecho público entre sus amigos de esta incursión informática una vez lograda, sin darse cabal cuenta que estaba marcando rumbos en la seguridad informática mundial. ¿Cómo se

[6] Qiao Liang y Wang Xiangsui, Unrestricted Warfare, Pan American Publishing Company, Panama, 2002, P. 34.
[7] Ibídem, passim.

puede lidiar con los *hackers* que van y vienen como sombras en Internet usando este mismo tipo de método?

Estos *hacker* alteraban los programas o enviaban malware, códigos maliciosos que se introducen en las computadoras o sistemas de información para generar daños. No es propósito de este ensayo abundar sobre estos aspectos, sino decir que en general incluyen distintos tipos de virus como troyanos, gusanos, bombas lógicas, hoax, rootkits y spyware. Nació así la necesidad de desarrollar la seguridad informática, que en un inicio se concebía como la disciplina que relaciona diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios. Al efecto, surgieron los antivirus conocidos, y los firewalls.

Los apuros para conseguir mercados aumentaron las vulnerabilidades. Los sistemas operativos eran comercializados en una carrera contra el tiempo, y el software era incompleto y con defectos, que se solucionaban más tarde (parches para *bugs*), o con nuevas versiones. Es así que desde el punto de vista de seguridad informática, Windows de MSN e Internet Explorer tienen mucho más agujeros de seguridad que otros sistemas operativos y navegadores, por ser más conocidos y usados.

La Seguridad Informática Estatal

Si bien el terreno de la informática y las telecomunicaciones es global, los Estados tienen responsabilidad soberana sobre esos medios dentro de su territorio. Hoy, la Seguridad Informática es la componente más sensible de la seguridad estatal puesto que se amenaza a los sistemas financieros nacionales, a la infraestructura industrial de un país, a los sistemas de salud, de transporte, a los sistemas de seguridad social, y al abastecimiento de energía interconectada. Puede paralizarse el sistema bancario de un país, destruir instalaciones clave mediante ataques cibernéticos y tener acceso a información secreta y de muy alta importancia para la Defensa Nacional. Inadvertidamente, la vida diaria depende del uso de programas de computación: el abastecimiento de electricidad, la apertura de las compuertas de las usinas hidroeléctricas, los proyectiles nucleares, las centrales nucleares, el control del tráfico aéreo, hasta la impresión de los diarios.

Es así como el uso del espacio cibernético comenzó a ser preocupación de los Estados. Ya no se trataba únicamente de fraudes con tarjetas de crédito, o pornografía infantil usando internet, mediante correos electrónicos – a lo que se denomina Seguridad Cibernética para enfrentar al delito cibernético - sino lo que estaba en riego era la seguridad de los Estados – a lo que se denomina Defensa Cibernética. Ya no se trataba de interferir correos electrónicos, ocupar espacio en las memorias RAM, o agregar o sacar datos de computadoras con fines delictivos. Se trataba de un problema de *defensa cibernética nacional*, porque se encontraba ante un *ataque cibernético* deliberado contra la estructura de un Estado, con efectos tan devastadores como si se hubiese tratado de un ataque nuclear. Estamos en el dominio de la Guerra Cibernética, una guerra no convencional, donde una agresión no necesariamente significa invasión del territorio nacional.

Llegado a este punto, los mayores de 50 años entran en el terreno de la ciencia ficción. Así como los ancianos de 1969 siempre dudaron que en realidad el hombre hubiese llegado a la Luna, hoy se duda que se pueda generar un desastre nacional desde una computadora en las antípodas. Eso fue así hasta que ocurrió el caso de Estonia en el 2007.[8]

El 27 de Abril del 2007, Estonia fue atacada cibernéticamente. En pocas horas, los portales web de los principales bancos de Estonia colapsaron. Todos los sitios web de los periódicos, dejaron de circular y publicar noticias; las comunicaciones de los órganos de gobierno de Estonia cesaron en sus comunicaciones. Un enemigo había asaltado docenas de blancos en el país. Esto, no obstante, no había sido resultado por un ataque de armas químicas, biológicas, nucleares o de destrucción masiva; tampoco fue por un ataque terrorista sino por una red de computadoras. Este pequeño Estado de Europa era el más informatizado, tanto que jocosamente se lo llama eStonia. Estonia había establecido un sistema de gobierno basado en la informática: el 90% de los servicios de los bancos y hasta las elecciones parlamentarias, se llevaban a cabo por Internet. Se paga el estacionamiento y los impuestos por teléfonos móviles, y se pueden realizar compras a través de ellos. El país está saturado de Wi-Fi. Así Estonia es considerada una ventana al futuro, y en algún día, todos los países serán como Estonia. Esto contribuyó a la efectividad del ataque cibernético.

[8] From Nuclear War to Net War: Analogizing Cyber attacks in International Law, P. 191

En cuestión de días, los ataques cibernéticos hicieron colapsar los sitios web más críticos del Estado y eso trajo consigo muchísimos desordenes sociales, heridos y un muerto. Nunca antes un país había sido atacado cibernéticamente en todos los frentes de una sola vez. El Ministro de Defensa de Estonia pensó en invocar el Art. 5 de la carta de la OTAN, como seguridad colectiva. Se atribuyó a Rusia la autoría de este ataque cibernético, como venganza a un acto de vandalismo sobre el monumento al Soldado Desconocido Soviético de la ciudad de Tallín, llevado a cabo por manifestantes estonios. El ataque cibernético no fue completo, ya que los servicios de agua, electricidad, cloacas, policía y bomberos, y transporte aéreo no fueron atacados. Probablemente haya sido la primera prueba piloto de un ataque cibernético a un Estado, por parte de otro Estado.

En Agosto de 2008, otro ataque cibernético tuvo lugar en Georgia previo a la invasión rusa a Ossetia del Sur, donde el contenido de las páginas web de las Agencias de Información fue modificado. La inteligencia rusa fue acusada, pero negó tal cargo aunque su participación era altamente probable.

En Noviembre de 2010 Irán reconoció que dos de sus plantas nucleares fueron atacadas por un virus informático tipo gusano llamado *Stuxnet* que había afectado los controladores de Siemmens que las regulaban. Esta vez fue Israel el Estado acusado. El último virus desarrollado, el más pernicioso, se denomina *Flame* y tiene la característica que la ingeniería reversa para hallar el virus en un archivo infectado es sumamente dificultoso porque el *Flame* borra las transacciones luego de un tiempo. Además, es un virus tipo gusano que puede recibir instrucciones adicionales luego de ser instalado. Se ha difundido principalmente en Medio Oriente, pero la mayoría de los blancos están en Irán. Sus creadores permanecen en el anonimato.

El 8 de Marzo de 2011 los diarios publicaron que Francia había sufrido un ataque cibernético. El Ministerio de Economía y Finanzas informó de un ataque que logró infiltrar

durante varias semanas unas 150 computadoras de dos áreas cruciales: la de los servicios del Tesoro -que también es responsable del Club de París- y la base de datos del G-20.[9]

El marco legal de los ataques cibernéticos es incipiente. Las políticas públicas de los Estados respecto a la agresión cibernética, también están en bajo grado de desarrollo. Según los técnicos, solo el respaldo de un Estados brinda los recursos necesarios para llevar a cabo un ataque cibernético de envergadura contra otro Estado. En su momento, Rusia hizo público sus reservas de usar armas nucleares contra ataques informáticos. En forma similar, las administraciones de Clinton y Bush han equiparado los peligros de la Guerra Cibernética con el efecto de las armas de destrucción masiva.

La información sobre la agresión cibernética no es totalmente pública. Incluso algunos artículos técnicos tienen una advertencia, que indica que se le ha suprimido información sensible.[10] Los límites entre el delito cibernético, el terrorismo cibernético y el ataque cibernético no son claros, por lo que toda estrategia nacional de defensa cibernética debe ser integral. La división convencional entre ataque y defensa, se difumina.

Una de las características de estas agresiones cibernéticas es el anonimato. Como se publicita abiertamente en Internet, el anonimato no es delito. Técnicamente, se pueden usar *proxies* que oculten el origen del ataque, la piratería o el delito. [11]Ahora se duda sobre el bombardeo a la Embajada de China en Belgrado el 7 de mayo de 1999 que se atribuyó a un daño colateral no deseado, causado por aviones de Estados Unidos. En realidad no habría sido otra cosa que una represalia por el derribo del primer F-117 Stealth en teoría invisible al radar, por parte de fuerzas serbias el 27 de marzo de ese año fue, con información electrónica que le habría sido proporcionada a Serbia por la Embajada China en Belgrado. Alguien puede dudar de esta relación fáctica pero no puede negarse que las fechas son notoriamente próximas.

---

[9] Link http://www.lanacion.com.ar/1355666-el-gobierno-de-francia-victima-de-un-ciberataque

[10] Kevin Coleman, 2008 Cyber Warfare Doctrine Addressing the most significant threat of the 21st century Public Version Sensitive Security Information Removed, The Technolytics Institute 6/1/2008 disponible en http://www.findthatpdf.com/search-2753509-hPDF/download-documents-Cyber-Warfare-Doctrine-Public-Version.pdf.htm. Hoy este documento no se encuentra disponible, fue removido de la web.

[11] Programas para servers anónimos que ocultan el IP son de público acceso en Internet: *JonDo* se instala y se activa cuando se necesita. También hay páginas web que permiten hacer anónima la navegación como *anonimizer, anonimouse, somebody, ivacy, masked Ip, hide-my-ip*, y otros. Son de acceso público.

Del mismo modo en la Guerra del Golfo, los aliados habrían enviado *drones* con supresores de frecuencia para que los captasen las pantallas del radar antiaéreo. Los sistemas de defensa aérea se dividen en radares de adquisición y radares de tiro interconectados: las piezas antiaéreas se apuntan automáticamente. Operando como un sistema de computación, las pantallas de radar de adquisición se comportan como un periférico: si se anula la frecuencia de los motores de los jets de ataque, los radares solo captarán las turbinas de los vuelos comerciales. Es un problema de detección de frecuencias, como ocurre con el número de aspas de las hélices de los submarinos. Tal parece que así ocurrió, pero seguramente esto permanecerá por mucho tiempo en duda.

El futuro

Lo más probable es que la amenaza cibernética, en sus formas de *delito cibernético*, *terrorismo cibernético* y *ataque cibernético* llame la atención de las Naciones Unidas. Probablemente se pida a los Estados políticas públicas al respecto, y se deba formular Estrategias de Seguridad y Defensa del Ciberespacio nacionales. Seguramente se requerirá un alto grado de cooperación e integración regional como herramienta para combatir a las amenazas cibernéticas. Aquí surgirá irremediablemente la discusión si el hecho de un ataque cibernético a un Estado lo autoriza al ejercicio del derecho de defensa propia del Art. 51 de la carta ONU.

Muchos adelantos tecnológicos se desarrollaron simultáneamente, los chips, microchips, fibras ópticas, procesadores, servers, computadoras y los nanoprocesadores de reciente aparición. Todas estas innovaciones se reunieron y aceleraron mutuamente, significado de sinergia: el resultado es superior a la simple suma. La tecnología va por delante de la comprensión. En Estados Unidos, la mayoría de las operaciones comerciales se realizan por Internet, facilidad que en el año 1996 era una expresión de deseo. La gente con más de 50 años de edad no cree que su celular, además de funcionar como teléfono móvil, sea un dispositivo GPS. El GPS, que hace 15 años era notoriamente voluminoso, y hoy puede instalarse en un reloj pulsera. Existen programas que permiten ubicar a las personas a través de su teléfono móvil, y esa facilidad se asocia a los recursos de Internet, como el caso de *Google Latitude*. Otro de los aspectos que resulta más perjudicial es el hecho que todo el software relacionado con esta temática puede conseguirse en el mercado negro, y al alcance de cualquiera que pueda pagarlo.

En curso está el conocido sitio Wikileaks [12] Este sitio revela documentos secretos de todos los países, y el sitio está disponible en múltiples servidores con diferentes nombres de dominio luego que su dominio original fuera atacado desde diferentes sistemas de servidores para negarles el servicio de *hosting*.

Los Estados deberán estar en condiciones de defenderse de ataques cibernéticos, y de no permitir que sus facilidades de informática y telecomunicaciones sean usadas por terceros estados como trampolín. Esta defensa puede implementarse a través del desarrollo de ataques cibernéticos y dar lugar a la vigencia de lo dicho por Clausewitz: *una defensa no es sino un escudo compuesto por golpes bien dirigidos.*

Hoy resultaría ridículo pensar que la Central Nuclear de Atucha está bien protegida porque tiene una defensa física policial a través de un cordón perimetral. Quien así piense, todavía esta viviendo en el siglo pasado. Si el ataque cibernético es una agresión estatal estratégica, no tendría sentido tratarla con los medios preparados para enfrentar el delito común cibernético, sino en el ámbito de la Defensa Nacional. Por eso es necesario elaborar una Estrategia Nacional de Seguridad y Defensa Cibernética, y cooperar internacionalmente

El ser humano ha creado un monstruo de varias cabezas, y ahora quiere regular su sinergia. Por de pronto, la guerra cibernética es como dijeron los pensadores militares desde hace mucho tiempo: *no hay guerra parecida a la anterior*.

[12] http://wikileaks.org/