StuxNet – El *software* como herramienta de control geopolítico

StuxNet – El software como herramienta de control geopolítico

Francisco Silva G.[1]

Recibido: 21 de diciembre de 2017
Aceptado: 31 de enero de 2018

[1] Universidad de Buenos Aires, Especialista en Seguridad Informática, Buenos Aires, Argentina (fcosilva@riseup.net).

StuxNet – El *software* como herramienta de control geopolítico

StuxNet – El software como herramienta de control geopolítico

Francisco Silva G.

Palabras clave: *Stuxnet*, virus, *software*, geoplítica, control, poder, SCADA, Linux, *Microsoft*, ciberguerra.

Keywords: Stuxnet, virus, software, geopolitics, control, power, SCADA, Linux, Microsoft, cyberwar, Iran, Israel, United States, malware, zero day.

Resumen

Las tecnologías evolucionan rápidamente, y esta carrera no deja atrás al *malware*. En el 2010 se dio a conocer un virus informático que marcó un hito por sus efectos que cruzan la línea entre lo virtual y el mundo real, y por conjugar además elementos tecnológicos y geopolíticos, dando luz de lo que podrían ser las próximas guerras. El virus *StuxNet* atacó con éxito infraestructura crítica de un país de Medio Oriente dejando rastros que describen un contexto geopolítico del que formó parte, y que ha dado origen a múltiples investigaciones las cuales han servido para la elaboración de este artículo. El caso *StuxNet*, plantea a la soberanía tecnológica de importancia estratégica para un país, es decir, el tener control sobre las tecnologías, y generar capacidad técnica local para lograrlo.

Abstract

Technologies evolve fastest and it doesn't leave malwares behind. In 2010, a computer virus appear that marked a milestone due to its effects that eliminated the frontiers between the virtual and real world. At the same time, this virus combined technological and geopolitical elements that would allow know how coud be the next wars.

StuxNet virus successfully attacked critical infrastructure in Middle Eastern, leaving traces that describe a geopolitical context which was a part of it. This context motive a lot of researches that were used for this articule.

The StuxNet case stand out the strategic importance of technological sovereignty for a country, that means having control of technologies, and generating local technical capacity to achieve it.

Introducción

En junio de 2010, una ciberamenaza fue descubierta de manera accidental por investigadores de una pequeña empresa bielorussa llamada VirusBlockAda. Esta amenaza informática, conocida como *software* malicioso (*malware*), se propagaba infectando memorias Pen Drive USB. Lo particular de este *malware* es el interés y la preocupación que despertó en los expertos de seguridad a medida que se lo iba analizando, dado el nivel de sofisticación y de estragos que era capaz de producir, marcando un hito en la historia de las ciberamenazas.

El virus de nombre *Stuxnet* fue considerado una revolución en asuntos militares (RMA)[1] por trasgredir los límites de lo virtual produciendo estragos en el mundo real, lo cual supuso un giro en la naturaleza del concepto de ciberguerra. Como resultado, se produjo la afectación de equipos industriales, con pruebas

[1] La RMA (Revolution in Military Affairs) revolución en asuntos militares, es un término utilizado por primera vez en el "Informe Anual del Secretario de Defensa al Congreso de los Estados Unidos" en 1998, término que proviene desde los 80s por el Mariscal de la Unión Soviética Ogarkov como MTR (Military Technical Revolution) que sostenía que con el empleo de las nuevas tecnologías de la información, sensores y reconocimiento electrónico, se podía garantizar una victoria militar frente a oponente fuertemente armados físicamente.MOLINA R., David, «La Revolución de los Asuntos Militares (RMA) en el contexto de la era de la información», *Ámbitos* (2005): 77-85, http://helvia.uco.es/xmlui/bitstream/handle/10396/10563/7.pdf?sequence=1.

que indican que se cumplieron los objetivos del virus, poniendo de manifiesto un adelanto significativo en el desarrollo de *software* maliciosos, por las consecuencias producidas.[2]

Los primeros análisis (posteriores a junio 2010) indicaban que el virus pudo haber estado trabajando sigilosamente durante meses e incluso años antes de su descubrimiento público. No se puede determinar si es el primer *software* malicioso que afecta a equipos industriales, puesto que existieron antecedentes en la década de 1980 (como el caso del gaseoducto Siberiano[3]), pero sí se puede afirmar que es el primer *gusano informático*[4] que aprovechó la vulnerabilidad reportada en el boletín MS10-046[5] de los sistemas operativos Windows. Los sistemas y programas, fabricados por la marca alemana Siemens, que se emplean en los sistemas SCADA (*Supervisory Control and Data Acquisition*) utilizan Windows como sistema operativo. Estos sistemas constituyen la plataforma para controlar y automatizar infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales.[6]

Este tipo de *software* malicioso no utiliza Internet como vector de ataque para propagarse[7], sino que lo hace a través de pen drive, es decir, memorias

[2] SHAKARIAN, Paulo. «*Stuxnet*: Revolución de Ciberguerra en los Asuntos Militares», *Air & Space power journal* (2010): 50-59, http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s.pdf.

[3] En 1982 explotó el gaseoducto transiberiano a causa de un *malware* informático que la CIA implantó en *software* canadiense utilizado por la exURSS (Unión Soviética) según información desclasificada por la CIA. «Update: Agent Farewell and the Siberian Pipeline Explosion», 2013, https://nsarchive.wordpress.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/.

[4] Los "gusanos informáticos" son un tupo de *malware* que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del sistema operativo. Este tipo de virus no requieren infectar a un archivo para realizar sus propósitos.

[5] MS10-046 es un boletín de seguridad publicado por *Microsoft* en agosto del 2010, en referencia a la vulnerabilidad CVE-2010-2568 de alta probabilidad de explotación. "La vulnerabilidad podría permitir la ejecución remota de código si se muestra el icono de un acceso directo especialmente diseñado. Un intruso que aprovechara esta vulnerabilidad podría conseguir el mismo nivel de derechos de usuario que el usuario local." «Boletín de seguridad de *Microsoft* MS10-046 - Crítica», 2010, https://technet.microsoft.com/library/security/ms10-046?f=255&MSPPError=-2147217396.

[6] SÁNCHEZ MEDERO, Gema. «La ciberguerra: los casos de *Stuxnet* y Anonymous», *Revista Derecom n.º 11* (2012): 124-133, http://derecom.com/numeros/pdf/gema.pdf.

[7] Un vector de ataque es el método o medio que utiliza una amenaza para atacar un sistema.«Glosario de Seguridad», accedido 28 de octubre de 2015, http://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad.

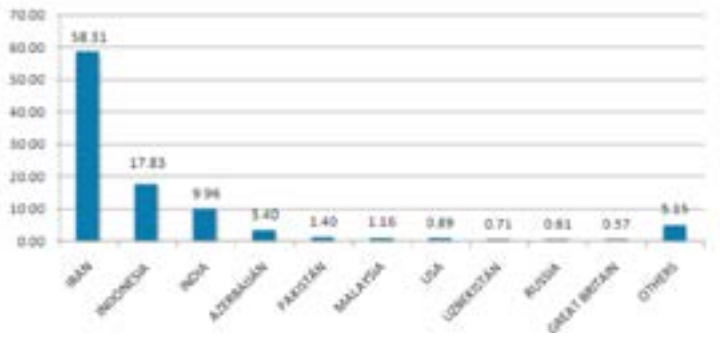
externas de tipo USB. *Symantec*, una de las empresas de seguridad que ha investigado el *malware*, detectó a finales de septiembre del 2010, 100.000 máquinas infectadas, de las cuales la gran mayoría (aproximadamente 60.000) se encontraban en Irán, seguido por Indonesia con 15.000 infecciones. En conjunto con otras empresas de seguridad, *Symantec* recopiló 3.280 ejemplares del *software Stuxnet* y variantes, lo que les permitió realizar un rastreo del historial de infección de una de las cinco organizaciones que fueron víctimas del *malware*.

Inevitablemente el virus se propagó y aunque hay informes del gusano en equipos SCADA[8] en Alemania, Finlandia y China, solo las infecciones en Irán produjeron daños a los sistemas industriales. Esto tiene sentido, ya que *Stuxnet* solo ataca en ciertos sistemas con configuraciones específicas de PLC[9] (Controladores Lógicos Programables).[10]

[8] SCADA (Supervisory Control and Data Acquisition) son sistemas de de control y adquisición de datos utilizados para el control y monitoreo de plantas o equipamientos industriales tales como sistemas para control de: flujo de agua, energía, petróleo, gas, transporte. Estos sistemas comprenden la transferencia de datos entre un computador central SCADA, una cantidad de unidades remotas y la terminal del operador.«Supervisory Control and Data Acquisition (SCADA) Systems», Technical Information Bulletin 04-1, October (2004): 76, https://scadahacker.com/library/Documents/ICS_Basics/SCADA Basics - NCS TIB 04-1.pdf.

[9] "Según lo define la Asociación Nacional de Fabricantes Eléctricos de los Estados Unidos un PLC – Programable Logic Controller (Controlador Lógico Programable) es un dispositivo digital electrónico con una memoria programable para el almacenamiento de instrucciones, permitiendo la implementación de funciones específicas como ser: lógicas, secuenciales, temporizadas, de conteo y aritméticas; con el objeto de controlar máquinas y procesos." «Manual Controlador Lógico Programable (PLC)», *Automación Micromecánica s.a.i.c* (s. f.): 84, http://www.microautomacion.com/capacitacion/Manual061ControladorLgicoProgramablePLC.pdf.

[10] RID, Thomas. «Cyber War Will Not Take Place», *Journal of Strategic Studies* 35, n.o 1 (2012): 5-32, doi:10.1080/01402390.2011.608939.



Distribución geográfica de la infección por *Stuxnet* [11]

Según las investigaciones recién mencionadas, probablemente *Stuxnet* fue instalado por un saboteador en Natanz utilizando una tarjeta de memoria USB. Estas conclusiones van de la mano con el anuncio que diera el Ministro de Inteligencia de Irán, Heydar Moslehi, en octubre del 2010, acerca de una cantidad no específica de "espías nucleares" arrestados en conexión con *Stuxnet*. Es decir, los diseñadores del gusano informático no esperaban una propagación inicial pasiva, sino que contaban con una infiltración directa del virus.

Es evidente que *Stuxnet* no intentaba hacer estragos inmediatamente, sino ocasionar el daño de manera sutil a través del tiempo ajustando las frecuencias de las centrifugadoras[12] paulatinamente, lo cual dificultaría detectar el origen del problema, al no poder determinar si el mismo se estaba produciendo por fallos en alguna parte del proceso de enriquecimiento.

[11] LEJARZA ILLARO, Eguskiñe, «Ciberguerra, los escenarios de confrontación.», 2014, 1-20. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf.

[12] El enriquecimiento de uranio es un proceso al cual es sometido el uranio natural que permite obtener una mezcla más rica de uranio 235, que se puede utilizar para fines civiles o militares. Una de las tecnologías utilizadas en este proceso son las centrifugadoras de gas.

Mecanismo de Ataque

En las plantas industriales o infraestructuras críticas, los operadores tienen que programar unos dispositivos llamados PLC (Controladores Lógicos Programables), que constituyen el componente de inteligencia de los equipos industriales, ya que estos reciben instrucciones de los PLC que determinan por ejemplo la apertura de una válvula, de una compuerta, o la frecuencia con que debe girar un motor.

Para programar los PLC, los operadores deben conectar temporalmente una computadora portátil. En el caso de los equipos *Siemens*, probablemente se utilizó el llamado *Field PG*, *notebook* industrial especializado vendido por la marca. A diferencia del sistema de control central y el propio controlador (PLC), estos PGs utilizan como sistema operativo *Microsoft Windows*, y lo más probable es que por la criticidad de los sistemas estos *notebook* no se los conecte a Internet o ni siquiera a una red interna.

Es aquí donde entra la ingeniería social como estrategia para hacer factible la infección, es muy probable que hayan intervenido agentes de inteligencia ("espías") para introducir *Stuxnet*, por medio de memorias USB, en el entorno de destino donde luego se extendió en el interior con el fin de alcanzar su objetivo deseado y preciso. Desde el primer objetivo, que fue lograr introducir el virus dentro de las instalaciones, hasta que este se haya logrado expandir y conseguir infectar los *notebook* que se utilizan para programar los PLC, debió pasar cierto tiempo. El mecanismo de infección del gusano tenía que ser agresivo, por lo que el número de infecciones colaterales y sin importancia fue inicialmente grande.

La estrategia de sabotaje de *Stuxnet*, como lo describe *Symantec*, es su complejidad y especificidad. El objetivo final era afectar dos modelos de controladores lógicos de Siemens (PLC), el 6ES7-315-2 y el 6ES7-417, abreviados como código 315 y 417 respectivamente. Los objetivos probables fueron las turbinas K-1000-60 / 3000-3 en la planta de energía nuclear de Bushehr que utilizaban el código 417 y las centrifugadoras en Natanz que tenían el modelo de código 315.

Si el *malware* lograba conectarse a dichos controladores (315 y 417), procedía a comprobar sus configuraciones para identificar si corresponden al equipo industrial objetivo. Si *Stuxnet* no encontraba la configuración correcta, se mantenía en estado latente. Pero si encontraba la configuración objetivo que correspondía a las centrifugadoras, el gusano atacaba.

Estas cargas útiles, es decir, la parte maliciosa del código de *Stuxnet* que ejecutan los ataques específicos, tenían la tarea de cambiar las frecuencias de salida de controladores determinados (315, 417) que ejecutan motores. *Stuxnet* se creó para provocar mal funcionamiento de procesos industriales, daños físicos a rotores, turbinas, y centrífugas.

El objetivo final del ataque era dañar las centrifugadoras lentamente, no de manera inmediata, logrando engañar a los operadores de la planta. Perjudicar el *hardware* retrasaría el programa de enriquecimiento de Irán por un período importante, considerando que los componentes dañados no se pueden adquirir fácilmente en mercados abiertos, el ataque sería estratégicamente muy valioso.

Otro elemento estratégico del ataque perpetrado por *Stuxnet*, es la clandestinidad. Una vez que *Stuxnet* alcanza infectar el *notebook* de operación de los PLC, antes de iniciar el sabotaje per se, primero se dedica a recabar información. Intercepta valores de entrada de los sensores (por ejemplo, el estado de una válvula o temperaturas de operación) con el fin de registrar esos datos, almacenarlos y luego utilizarlos para engañar al operador.

El *malware* actuaba como un intermediario entre el *software* que utilizaba el operador para programar los PLC y el equipo industrial. Es decir, enviaba las instrucciones del *software* manipuladas e incorrectas al equipo industrial y a su vez devolvía al *software* del controlador señales de entrada falsas, que previamente había registrado y almacenado de un funcionamiento normal antes de iniciar el ataque. Esto era realizado con el fin de engañar a los operadores en la sala de control haciéndoles creer que las configuraciones correctas habían sido cargadas. Además estos veían en sus paneles de monitoreo central valores que respondían a los parámetros esperados.

Adicionalmente, *Stuxnet* escondía las modificaciones y manipulaciones que enviaba a la controladora, violando los sistemas de seguridad digitales. Incluso el *malware* tenía mecanismos para evadir el antivirus, y ocultarse o autoeliminarse en caso de no lograr su propósito.

Ralph Langer, consultor alemán en Seguridad de Sistemas de Control, parte del grupo de ingenieros que decompiló[13] el virus, argumentó que "los recursos e inversiones realizados para *Stuxnet* pudieron solo ser reunidos por una súper potencia cibernética". Una posibilidad sería que Israel con soporte de EEUU haya estado detrás de la amenaza.

[13] Es un método utilizado en la ingeniería inversa de *software*, para generer o recrear el código fuente de un lenguaje de alto nivel, a base de un programa ya compilado (ejecutable).

Otro elemento de inteligencia para analizar es que el atacante necesariamente debió tener acceso de información precisa y de primera mano de los esquemas específicos del sistema de control objetivo.[14] Para esto debieron haber robado o extraído el diseño (un mecanismo sería utilizando una versión anterior de *Stuxnet*), o pudieron simplemente solicitarlos al fabricante de manera colaborativa. Haciendo alusión al arduo trabajo de inteligencia, Langner con cierto humor afirma "probablemente sabían la talla de zapato del operador".[15]

Respecto a los recursos utilizados o invertidos para asegurarse que el ataque fuera exitoso, es decir, reducir al mínimo las probabilidades de falla, y considerando el nivel de especificidad del ataque, es probable que los atacantes hayan tenido que configurar un ambiente similar para depurar su vehículo de ataque, lo que significa haber montado una instalación simulada de enriquecimiento.

Mientras más se profundiza en el análisis del *malware*, más se ponen en evidencia ciertos supuestos que delatan patrones, objetivos, propósitos e incluso perpetradores. Es evidente que programar tal complejidad requiere no solo mucho tiempo, sino recursos, y un equipo avanzado de programadores que incluye además personal y procesos de gestión de calidad de *software*, es decir, un ciclo completo de desarrollo de *software*.

Los programas maliciosos o *malware*, como *Stuxnet*, para poder atacar requieren apuntar a fallos del sistema operativo (bugs) que no hayan sido descubiertos, lo que en el mundo informático se le denomina vulnerabilidades de "día cero" (zero-day exploits). Estas son fallas en los sistemas que no han sido descubiertas, o ya lo fueron pero no son públicas o conocidas, sino tan solo por expertos que comercializan con esta información, o incluso el mismo dueño del *software* para propósitos estratégicos. Esto quiere decir, que las 4 vulnerabilidades de "día cero" utilizadas por *Stuxnet*, elementos difíciles de conseguir, debieron costar una suma importante de dinero, si es que no fueron proporcionadas directamente por la empresa dueña del *software* (*Microsoft*).

Además como parte del proceso de ocultamiento del virus, *Stuxnet* debió utilizar certificados digitales del *software*

[14] Cada equipo y sistema industrial trabaja con un conjunto de valores específico que va a depender de ciertos factores como son la marca, el modelo, incluso la utilización determinada que en conjunto podrán definir configuraciones únicas.

[15] RID,Thomas, «Cyber War Will Not Take Place», 35.1 (2012), 5-32

de la controladora robados a los fabricantes de *hardware* JMcron y Realtek. Está de más decir que se trata de un sabotaje informático de gran escala.[16]

¿Una ciberoperación?

La compañía de Seguridad Informática *Symantec* califica a *Stuxnet* como "el primer virus informático que permite hacer daño en el mundo físico"[17]. A base de esto ¿hasta qué punto se podría considerar este caso como una ciberoperación que derive a un "ataque armado", o hasta qué punto se lo puede considerar como una ciberarma?

Según las interpretaciones del Manual de Tallín del Derecho Internacional, se podrían considerar como "ataque armado" a los ciberataques que hieren, matan o destruyen propiedades, y no a aquellos que guardan relación con inteligencia, robo y, en general, aquellos que no interrumpen servicios esenciales (un hipotético ataque a una central distribuidora de agua para envenenamiento y que provocara enfermedades, no hay duda de que sería un ataque armado).[18]

Sin embargo, la realidad es que ningún ataque cibernético ha sido considerado al día de hoy, como ataque armado, a pesar que el caso de *Stuxnet* (a diferencia de otros casos como el de Estonia[19]) parece haber alcanzado el umbral para ser considerado como tal, pues produjo la paralización del programa nuclear iraní, siendo además el uso de medios informáticos que produjo efectos similares al que haría un bombardeo por parte de una nación en contra de otra.

Según el análisis de T. Rid (2012), "un acto ofensivo debe reunir ciertos criterios con el fin de calificar como 'acto de guerra'. Cualquier acto de guerra debe tener el potencial de ser: letal (violento),

[16] SÁNCHEZ MEDERO, Gema, «*La ciberguerra: los casos de Stuxnet y Anonymous.*»

[17] LEJARZA ILLARO, Eguskiñe, «Ciberguerra, los escenarios de confrontación.»

[18] REGUERA SÁNCHEZ, Jesús. «Aspectos legales en el ciberespacio . La ciberguerra y el Derecho Internacional Humanitario» (2015): 1-30.

[19] "En Estonia las páginas oficiales de varios departamentos estonios, las del gobierno y las del gobernante Partido de las Reformas quedaron paralizadas por ataques informáticos provenientes del exterior. Al mismo tiempo que los sistemas de algunos bancos y periódicos resultaron bloqueados durante varias horas por una serie de ataques distribuidos de denegación de servicio (DDoS), hecho que se produjo justo después de que Rusia presionara a Estonia por la retirada de las calles de Tallin de un monumento de la época soviética." SÁNCHEZ MEDERO, Gema, «La ciberguerra: los casos de *Stuxnet* y Anonymous.»

tiene que ser instrumentado, y tiene que ser político"[20]. A base de esta definición, Rid afirma que ninguno de los casos ofensivos cibernéticos constituyen un acto de guerra por sí mismos.

De acuerdo con Rid, toda guerra es violenta y por lo tanto letal, además la guerra tiene carácter instrumental, es decir, debe tener un medio y un fin. El uso de la fuerza, o la violencia física es el medio, el fin es forzar al enemigo a aceptar los objetivos impuestos por el contrincante. Además la guerra es de naturaleza política, es decir, nunca es un acto aislado, "es la mera continuación de la política por otros medios"[21]

Para su análisis, este autor considera tres tipos de delitos: subversión, espionaje y sabotaje; actividades que pueden involucrar actores estatales o no estatales (privados).[22] Todos los casos de ciberataques o delitos cibernéticos entran en esta clasificación, y el caso de *Stuxnet* encajaría en la tipología de sabotaje, independientemente de haber sido perpetrado con medios informáticos.[23]

Se entiende por sabotaje, al intento deliberado de debilitar o destruir un sistema económico o militar. El sabotaje es predominantemente de naturaleza técnica, pero por supuesto puede utilizar otros recursos como ingeniería social. Si en el sabotaje es usada la violencia, el objetivo primario deben ser los objetos no las personas.[24]

El punto clave del análisis es que el sabotaje ejecutado por *Stuxnet* no estaba conectado a una operación militar convencional, aparentemente. Las empresas de seguridad catalogaron a *Stuxnet*, como una amenaza persistente avanzada (APT[25]). Sin embargo, por los análisis realizados *Stuxnet* fue una campaña de varios años, es decir, se estima que el programa se inició a finales de 2007 o inicios de 2008, y además hay indicios que el ataque principal habría sido ejecutado entre junio de 2009 y junio de 2010, fecha en la que empresas de segu-

[20] RID, Thomas, «Cyber War Will Not Take Place.»

[21] Ibid.

[22] Ibid.

[23] El fin último del virus *Stuxnet* fue afectar a las centrifugadoras de uranio, con el objeto de producir daños irreparables en dichos equipos que interrumpan el programa nuclear. Efecto similar al que hubiera producido un operador manipulando intencionalmente los equipos para los mismos efectos.

[24] Ibid.

[25] Un conjunto de procesos informáticos que actúan de manera sigilosa, invasiva y continua, apoyada por los gobiernos, los terroristas y grupos de cibercrimen bien financiados, programadas para enfocarse en una entidad específica en la propiedad intelectual, los diseños militares y otros valores corporativos.

ridad de tecnología de la información hicieron pública la existencia del gusano informático. Gracias a ciertas técnicas informáticas los ingenieros pudieron ser capaces de construir un historial de la infección del gusano, además del análisis de código del virus producto de aplicar ingeniería inversa, para poder analizar la amenaza, entender su funcionamiento y, en consecuencia, su propósito.[26]

Conclusiones

Como lo plantea Reguera, "Aunque a fecha de hoy no se tengan datos empíricos reales sobre los efectos de las ciberarmas, solo algunos hechos como los de Estonia (2007) y *Stuxnet* (2010), se cree que no es ciencia ficción y que sus posibilidades pueden ir más allá de una denegación de servicio[27]".[28]

Definitivamente *Stuxnet* llegó a convertirse en una celebridad tecnológica en la geopolítica de los ataques cibernéticos. Es el rockstar en un mundo donde las ciberarmas cobran complejidad y capacidades destructivas sofisticadas. No se puede negar que el *software* malicioso se ha perfeccionado progresivamente hasta llegar a la relevancia del célebre *Stuxnet*, pionero en ataques dirigidos contra importantes instalaciones industriales.

El dominio del ciberespacio debe considerarse como una dimensión transversal a los otros cuatro dominios reconocidos por los gobiernos (tierra, mar, aire, espacio). A diferencia de los otros cuatro dominios, el ciberespacio fue creado por el ser humano y no debe mezclarse, no son de naturaleza homóloga, de hecho el dominio del ciberespacio es vulnerable a la interrupción generalizada producida por el ser humano. Adicionalmente el dominio del ciberespacio es multidimensional, es decir, no posee límites o fronteras, en su dimensión virtual, sin embargo la infraestructura tecnológica que constituye su dimensión física está sujeta a leyes que enmarcan una soberanía. Cualquiera de estas dimensiones vulne-

[26] RID, Thomas, «Cyber War Will Not Take Place.»

[27] Un ataque de Denegación de Servicio (DoS) implica una acción o conjunto de acciones ejecutadas por una entidad maliciosa con el objetivo de provocar la no disponibilidad de un recursos determinado.ABLIZ, Mehmud, «Internet Denial of Service Attacks and Defense Mechanisms» March (2011): 1-50, http://people.cs.pitt.edu/~mehmud/docs/abliz11-TR-11-178.pdf.

[28] REGUERA SÁNCHEZ, Jesús. «*Aspectos legales en el ciberespacio . La ciberguerra y el Derecho Internacional Humanitario.*»

radas pueden afectar no solo a infraestructuras críticas o servicios militares, sino también a los servicios gubernamentales, civiles o comerciales.

El mercado de las nomenclaturas o etiquetas ha inventado el término ciberguerra, como una intensión de mercadear la guerra a las nuevas tendencias tecnológicas, es decir, un recurso más para hacer la guerra. Entonces, así como la ciberguerra, perpetrada en el ciberespacio ¿podríamos hablar también de aeroguerra, marguerra? o podríamos inventarnos las terminologías o excusas necesarias para legitimar ofensivas en el mundo virtual que deriven al mundo real. Sin duda podemos hablar de ciberseguridad, de ciberataques que son términos más adecuados para cualquier caso, y que constituyen un recurso más en una guerra.[29]

Según Kaspersky, empresa de seguridad informática "Hoy en día hay tres tipos conocidos de actores que desarrollan programas maliciosos y programas espía: los hacktivistas, los ciberdelincuentes y los gobiernos."[30]. Por las evidencias encontradas como resultado del análisis de los hechos y del *malware*, está claro que es un gobierno con el poder tecnológico y económico suficiente quien ha financiado toda la investigación necesaria para su desarrollo, ya que no se trata de un tipo de *malware* destinado a la infección masiva de computadoras domésticas, sino que están pensados para atacar un programa concreto de la marca Siemens (sistema SCADA) que se utiliza para controlar las infraestructuras críticas, que permiten aumentar o disminuir el caudal de un oleoducto o dañar una central nuclear.

Si se dejan a un lado todo el análisis y las conjeturas, un artículo publicado en el diario *The New York Times* en 2011 asegura que efectivamente se construyeron centrifugadores idénticas a las que tenía Irán, y que el virus se diseñó en las instalaciones secretas Israelíes de Dimona, en el desierto de Negev, donde se supone Israel desarrolla su propio programa nuclear.[31]

Este análisis también se pudo corroborar con las revelaciones del excontra-

[29] DOMBROWSKI, Peter & DEMCHAK, Chris C. «Cyber War, Cybered Conflict, and the Maritime Domain», Naval War College Review 67, n.o 2 (2014): 71-97, https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=94921561&site=ehost-live\nhttps://content-ebscohost-com.csuglobal.idm.oclc.org/ContentServer.asp?T=P&P=AN&K=94921561&S=R&D=aph&EbscoContent=dGJyMNHr7ESeqa44y9fwOLCmr0yeqK5SsKi4SLGWxWXS&ContentC.

[30] LEJARZA ILLARO, Eguskiñe, «*Ciberguerra, los escenarios de confrontación.*»

[31] BROAD, WIliam J, MARKOFF, John y SANGER, David E. «*Stuxnet* Worm Used Against Iran Was Tested in Israel», The New York Times, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?hp&_r=0.

tista de la NSA Edward Snowden, donde se confirma que efectivamente el *malware* fue creado en colaboración entre Israel y Estados Unidos, cuyo despliegue inició en el 2005 como parte de un programa llamado Operation Olympic Games, bajo la administración de Bush y continuado bajo la administración de Obama.[32]

Al tomar en cuenta el contexto geopolítico, se conoce la posición de Israel respecto a la proliferación de armamento nuclear en la región[33], lo que explica los actos de sabotaje por medio de ataques aéreos "preventivos" por sorpresa contra reactores nucleares de países como Irak, Siria, Sudan en Medio Oriente, por considerarlo como una amenaza contra su país. En el caso de Irán, la ruta aérea es más larga para Israel y está en una posición geográfica en la cual tendría que sobrevolar países neutrales, adicionalmente a esto las instalaciones de enriquecimiento de Irán se encuentran metros bajo tierra, por lo tanto el medio más efectivo para lograr un sabotaje exitoso era *Stuxnet*.[34]

Un detalle fundamental que hay que tomar en cuenta es el objetivo inicial de la infección. Este objetivo, que da puerta de entrada al sabotaje, es el sistema operativo *Windows* de *Microsoft* y sus 4 vulnerabilidades de "día cero". Es de conocimiento global, gracias a las revelaciones de 2013 de Edward Snowden[35], que *Microsoft* mantiene alianzas con la NSA (*National Security Agency*). Adicionalmente parte del *software* de *Microsoft* relacionado con su seguridad es desarrollado por Israel, lo que deja en sospecha la posibilidad de vulnerabilidades por diseño, y una estrecha colaboración entre este país y los EEUU a través de dicha organización. Entonces, suprimiendo esa variable de la ecuación (el sistema operativo) el ataque seguramente no hubiera sido posible.[36]

Se podría decir que *Stuxnet* fue un arma casi perfecta, a no ser por una falla en su código que permitió que se propagara masivamente por Internet. Los propios Iraníes reconocieron los daños provocados por el *malware*, que produjo retrasos en su programa nuclear, dejando fuera de servicio a un 20 % de las centrifugadoras.

Particularmente este caso, no fue perpetrado por medio de Internet, pues

[32] THOMSON, Iain. «Snowden: US and Israel did create Stuxnet attack code», The Register, 2013, http://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet/.

[33] http://www.eluniversal.com/opinion/150810/iran-israel-y-las-armas-nucleares

[34] Ibid.

[35] GREENWALD, Glenn, «Sin un lugar donde esconderse», Ediciones B, 2014

[36] SCHESTOWITZ, Roy. «The Lessons of Stuxnet: Never Use Microsoft Windows», Techrights, 2015, http://techrights.org/2015/05/30/stuxnet-in-northkorea/.

sería descabellado interconectar este tipo de infraestructura crítica a una red global. Esto demuestra que no necesariamente la *Internet* es un medio para perpetrar ataques de esta naturaleza, a pesar que las tendencias de querer conectarlo todo ha llegado a nuestro tiempo con el advenimiento del Internet de las Cosas (*Internet of Thing*).

El caso de *Stuxnet* no se hubiera dado con algo más de controles de seguridad física e informática, como probablemente sucedió con Corea del Norte, quienes a pesar de ser también objetivo del mismo ataque, este no tuvo éxito[37]; y sin duda alguna la soberanía tecnológica hubiera jugado un papel importante de protección si no se dependiera de sistemas propietarios fácilmente atacables por diseño como los sistemas operativos Windows[38] cuyo desarrollo de sus componentes de seguridad es realizado justamente por los países involucrados en la creación de *Stuxnet*.[39]

Los sistemas SCADA, los sistemas operativos, los motores de bases de datos, los sistemas de seguridad, de fabricación de las grandes marcas internacionales, todas o la mayoría de procedencia de las grandes potencias hegemónicas, dominan los mercados incluso la Internet que constituye el ciberespacio cuya dimensión física es soportada por *hardware* propietario que proviene de dichas potencias, que además controlan los flujos de información, así como la mayoría de normas y estándares tecnológicos internacionales. Entonces la soberanía tecnológica sin discusión juega un rol importante en la defensa.

[37] PUTZ, Catherine, «Why Did a US Cyber Attack on North Korea Fail?», accedido 11 de noviembre de 2015, http://thediplomat.com/2015/05/why-did-a-us-cyber-attack-on-north-korea-fail/.

[38] SCHESTOWITZ, Roy, «The Lessons of Stuxnet: Never Use Microsoft Windows.»

[39] THOMSON, Iain, «Snowden: US and Israel did create Stuxnet attack code.»

Bibliografía

Abliz, M. «Internet Denial of Service Attacks and Defense Mechanisms» n.o March (2011): 1-50. http://people.cs.pitt.edu/~mehmud/docs/abliz11-TR-11-178.pdf.

«Boletín de seguridad de *Microsoft* MS10-046 - Crítica», 2010. https://technet.microsoft.com/library/security/ms10-046?f=255&MSPPError=-2147217396.

Broad, Wlliam J., Markoff, J., y E. Sanger D. «Stuxnet Worm Used Against Iran Was Tested in Israel.» The New York Times, 2011. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?hp&_r=0.

Dombrowski, P., y Chris C Demchak. «Cyber War, Cybered Conflict, and the Maritime Domain.» *Naval War College Review* 67, n.o 2 (2014): 71-97. https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=94921561&site=ehost-live\nhttps://content-ebscohost-com.csuglobal.idm.oclc.org/ContentServer.asp?T=P&P=AN&K=94921561&S=R&D=aph&EbscoContent=dGJyMNHr7ESeqa44y9fwOLCmr0yeqK5SsKi4SLGWxWXS&ContentC.

«Glosario de Seguridad.» Accedido 28 de octubre de 2015. http://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad.

Greenwald, G. *No place to hide. IEE Review*. Vol. 51, 2014. https://cryptome.org/2014/05/npth-03.pdf.

Lejarza I., E. «Ciberguerra, los escenarios de confrontación.» (2014): 1-20. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf.

«Manual Controlador Lógico Programable (PLC).» *Automación Micromecánica s.a.i.c* (s. f.): 84. http://www.microautomacion.com/capacitacion/Manual061ControladorLgicoProgramablePLC.pdf.

Molina Rabadán, D. «La Revolución de los Asuntos Militares (RMA) en el contexto de la era de la información.» *Ámbitos* (2005): 77-85. http://helvia.uco.es/xmlui/bitstream/handle/10396/10563/7.pdf?sequence=1.

Rid, Thomas. «Cyber War Will Not Take Place.» *Journal of Strategic Studies* 35, n.o 1 (2012): 5-32. doi:10.1080/01402390.2011.608939.

Sánchez, J. «Aspectos legales en el cibe-

respacio . La ciberguerra y el Derecho Internacional Humanitario» (2015): 1-30.

Sánchez Medero, G. «La ciberguerra: los casos de *Stuxnet* y Anonymous.» *Revista Derecom* n.º 11 (2012): 124-133. http://derecom.com/numeros/pdf/gema.pdf.

Schestowitz, R. «The Lessons of Stuxnet: Never Use Microsoft Windows.» *Techrights*, 2015. http://techrights.org/2015/05/30/stuxnet-in-northkorea/.

Shakarian, P. «*Stuxnet*: Revolución de Ciberguerra en los Asuntos Militares.» *Air & Space power journal* (2010): 50-59. http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s.pdf.

«Supervisory Control and Data Acquisition (SCADA) Systems.» *Technical Information Bulletin* 04-1 n.o October (2004): 76. https://scadahacker.com/library/Documents/ICS_Basics/SCADA Basics - NCS TIB 04-1.pdf.

Thomson, I. «Snowden: US and Israel did create Stuxnet attack code.» *The Register*, 2013. http://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet/.

«Update: Agent Farewell and the Siberian Pipeline Explosion», 2013. https://nsarchive.wordpress.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/.

«Why Did a US Cyber Attack on North Korea Fail?» Accedido 11 de noviembre de 2015. http://thediplomat.com/2015/05/why-did-a-us-cyber-attack-on-north-korea-fail/.