Manifiesto Criptoanarquista

Cypherpunks del mundo,

En la reunión de 'Cypherpunks físicos', celebrada ayer en Silicon Valley, muchos de vosotros me pedísteis que estuviera disponible de forma electrónica más contenido del material que hemos aprobado en nuestras reuniones, para que pueda ser accesible y leído de forma completa por toda la lista de Cypherpunks, espías, curiosos y todo el que quiera.

Aquí está el "Manifiesto Cripto Anarquista" que leí en septiembre de 1992 en la reunión de fundación. Sus orígenes se remontan a mediados de 1988, cuando fue distribuido a algunos tecno-anarquistas afines en la conferencia "Crypto '88″ y de nuevo en la "Hackers Conference" de ese año. Posteriormente di charlas sobre esto en 'Hackers' en 1989 y 1990.

Hay algunas cosas que me gustaría cambiar, pero por razones históricas voy a dejarlo como está. Algunos de los términos pueden ser desconocidos para ustedes… espero que el Cripto Glosario que acabo de distribuir sea de ayuda.

(Esto debe explicar todos los términos criptográficos que hay en mi firma)

–Tim May

El manifiesto criptoanarquista

Un espectro está surgiendo en el mundo moderno, el espectro de la cripto anarquía.

La informática está al borde de proporcionar la capacidad a individuos y grupos de comunicarse e interactuar entre ellos de forma totalmente anónima. Dos personas pueden intercambiar mensajes, hacer negocios y negociar contratos electrónicos, sin saber nunca el Nombre Auténtico, o la identidad legal, de la otra. Las interacciones sobre las redes serán intrazables, gracias al uso extendido de re-enrutado de paquetes encriptados en máquinas a prueba de manipulación que implementen protocolos criptográficos con garantías casi perfectas contra cualquier intento de alteración. Las reputaciones tendrán una importancia crucial, mucho más importante en los tratos que las calificaciones crediticias de hoy en día. Estos progresos alterarán completamente la naturaleza de la regulación del gobierno, la capacidad de gravar y de controlar las interacciones económicas, la capacidad de mantener la información secreta, e incluso alterarán la naturaleza de la confianza y de la reputación.

La tecnología para esta revolución (y seguramente será una revolución social y económica) ha existido en teoría durante la última década. Los métodos están basados en el cifrado de clave pública, sistemas interactivos de prueba de cero-conocimiento, y varios protocolos de software para la interacción, autenticación y verificación. El foco hasta ahora ha estado en conferencias académicas en Europa y EE.UU., conferencias monitorizadas de cerca por la Agencia de Seguridad Nacional. Pero solo recientemente las redes de computadores y ordenadores personales han alcanzado la velocidad suficiente para hacer las ideas realizables en la práctica. Y los próximos 10 años traerán suficiente velocidad adicional para hacer estas ideas factibles económicamente y, en esencia, imparables. Redes de alta velocidad, ISDN, tarjetas inteligentes, satélites, transmisores Ku-Band, ordenadores personales multi-MIPS, y chips de cifrado ahora en desarrollo serán algunas de las tecnologías habilitadoras.

El Estado intentará, por supuesto, retardar o detener la diseminación de esta tecnología, citando preocupaciones de seguridad nacional, el uso de esta tecnología por traficantes de drogas y evasores de impuestos y miedos de desintegración social. Cualquiera de estas preocupaciones serán válidas; la criptoanarquía permitirá la comercialización libre de secretos nacionales y la comercialización de materiales ilícitos y robados. Un mercado computarizado anónimo permitirá incluso el establecimiento de horribles mercados de asesinatos y extorsiones. Varios elementos criminales y extranjeros serán usuarios activos de la CryptoNet. Pero esto no detendrá la extensión de la cripto anarquía. La cripto anarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes. Y de la misma manera que una invención aparentemente menor como el alambre de púas hizo posible el cercado de grandes ranchos y granjas, alterando así para siempre los conceptos de tierra y los derechos de propiedad en las fronteras de Occidente, así también el descubrimiento aparentemente menor de una rama arcana de las matemáticas se convertirá en el alicate que desmantele el alambre de púas alrededor de la propiedad intelectual.

¡Levántate, no tienes nada que perder excepto tus propias vallas de alambres con púas!

Timothy C. May