ALL TRANSLATIONS.

Fuentes.
http://chinalawtranslate.com/cybersecuritydraft/?lang=en

http://chinalawtranslate.com/user/jlvdaum/?lang=en

http://www.npc.gov.cn/

Ley De Seguridad Cibernética (Proyecto)

Por CLT En 06 de julio 2015 ·

Fuente:
http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm

La 15ª sesión del Comité Permanente de la 12 ª Asamblea Popular Nacional realizó la revisión inicial de esta "República Popular de Ley de Seguridad Cibernética China (Proyecto)" en junio de 2014. La "República Popular China Ley de Seguridad Cibernética (Proyecto)" Se lanzó a la pública en **la página web de la Asamblea Popular Nacional de China Congreso** para la recogida de los comentarios del público.

El público puede visitar directamente en el sitio web de la APN ((www.npc.gov.cn)) y formular observaciones, y también puede enviar comentarios **a Popular Nacional Congreso Jurídico Comisión de Trabajo,** (Pekín, Triciclos, Qianmen West Road # 1, 100,805) [en chino:**北京市西城区前**门西大街1号,邮编: 100805].

República Popular de Ley de Seguridad Cibernética China (proyecto)

Capítulo 1: Disposiciones Generales.

Artículo 1: Esta ley se formula a fin de garantizar la seguridad de la red, para preservar la soberanía ciberespacio, la seguridad nacional y el interés público de la sociedad, para proteger los derechos e intereses legítimos de los ciudadanos, personas jurídicas y otras organizaciones, y para promover el sano desarrollo de los derechos económicos e informatización social.

Artículo 2: Esta ley se aplica con respecto a la construcción, operación, mantenimiento y uso de las redes, así como la supervisión y gestión de redes en el territorio continental de la República Popular de China.

Artículo 3: El Estado persiste en la misma destacando seguridad de la red y el desarrollo de informatización, y se atiene a las directrices de uso positivo, el desarrollo científico, la gestión de acuerdo con la ley, y garantizar la seguridad; y avanza la construcción de la infraestructura de red, fomentar la innovación y la aplicación de tecnología de red, establecer y completar los sistemas de garantía de seguridad de red, y el aumento de la capacidad de proteger la seguridad de la red.

Artículo 4: El defensores estatales sincero, honesto, sano y civilizado comportamiento de la red, la adopción de medidas para aumentar la concienciación sobre la seguridad de la red de toda la sociedad y el nivel, y la formación de un buen ambiente para toda la sociedad a participar de manera conjunta en la promoción de la seguridad de red.

Artículo 5: El Estado lanza activamente el intercambio y la cooperación internacional en las áreas de gobierno ciberespacio, la investigación y el desarrollo de tecnologías de red, la formulación de normas, atacar la delincuencia informática y la ilegalidad, y otras áreas; promover la construcción de un ciberespacio pacífico, seguro, abierto y cooperativo.

Artículo 6:. La administración nacional ciberespacio es responsable de la planificación y coordinación de los esfuerzos de seguridad de red y supervisión y gestión de los esfuerzos relacionados integralmente El Ministerio de Industria y Tecnología de la Información, y la seguridad pública, así como otros departamentos pertinentes del Consejo de Estado, son los responsables de seguridad de la red protección, supervisión y gestión de esfuerzos dentro del ámbito de sus responsabilidades, de conformidad con las disposiciones de la presente Ley, las leyes y reglamentos administrativos.

De protección de la seguridad de red, supervisión y gestión de tareas para los departamentos pertinentes de los gobiernos de la gente a nivel de condado o superior serán determinadas por los reglamentos estatales pertinentes.

Artículo 7: La construcción y operación de redes o la prestación de servicios a través de redes deben estar de acuerdo con lo dispuesto en las leyes y reglamentos y los requisitos obligatorios de Estado o de estándares de la industria; la adopción de medidas técnicas y otras medidas necesarias para proteger la seguridad de red y la estabilidad operativa, de manera efectiva la respuesta a incidentes de seguridad de la red, prevención de los delitos cibernéticos, y salvaguardar la integridad, confidencialidad y capacidad de uso de los datos en línea.

Artículo 8: las organizaciones de comercio de la red relevantes son, de acuerdo con sus Estatutos Sociales, fortalecer la industria de la autodisciplina, formular normas de seguridad de red de comportamiento, guiar a sus miembros en el fortalecimiento de la protección de la seguridad de red de acuerdo con la ley, aumentar los niveles de protección de la seguridad de la red, y estimular el sano desarrollo de la industria.

Artículo 9: El Estado protege los derechos de los ciudadanos, personas jurídicas y otras organizaciones para utilizar las redes de acuerdo con la ley;que promueve el acceso a la red extendida, eleva el nivel de los servicios de red, proporciona servicios de red seguras y convenientes para la sociedad, y garantiza la circulación legal, ordenada y libre de información de la red.

Toda persona y organización serán, al utilizar la red, acatar la Constitución y las leyes, respetar el orden público y respetar la moral social, no deben poner en peligro la seguridad de la red, y no deben utilizar la red para participar en actividades que perjudican la seguridad nacional, la propagación del terrorismo y el extremismo, incitación al odio étnico y la discriminación étnica, la difusión de información obscena y sexual, calumniar o difamar a los demás, el orden social inquietante, perjudicando al interés público, infracción de la propiedad intelectual de otras personas u otros derechos e intereses legítimos.

Artículo 10: Todos los individuos y las organizaciones tienen el derecho de denunciar conductas poner en peligro la seguridad de red a los departamentos como para información de la red, la tecnología de la industria y de la información, la seguridad pública. Departamentos informes que reciben tramitarán con prontitud de conformidad con la ley; cuando éstas no caen dentro de la responsabilidad de ese departamento, se transferirá de inmediato el asunto al departamento de la facultad de manejar la situación.

Capítulo II: Red De Seguridad De Estrategia, Planificación Y Promoción.

Artículo 11: El Estado formula una estrategia de seguridad de la red, aclarando los requisitos básicos y principales objetivos de garantizar la seguridad de la red, poniendo adelante y mejorar los sistemas de salvaguardia de seguridad de red, aumentando la capacidad de protección de la seguridad de la red, estimular el desarrollo de la tecnología de seguridad de la red y la industria, y avanzar medidas de política para preservar la seguridad de la red con la participación de toda la sociedad, y así sucesivamente.

Artículo 12: Los departamentos del Consejo de Estado de Telecomunicaciones, la radio y la televisión, la energía, el transporte, la conservación del agua, las finanzas y otras industrias y otros departamentos pertinentes del Consejo de Estado deberá, sobre la base de la estrategia nacional de seguridad de la red, compilar los planes de seguridad de red relativos nacional la seguridad, las principales industrias de la economía nacional y la vida del pueblo, y los campos importantes, y organizar su ejecución.

Artículo 13:. El Estado establece y mejora de un sistema de normas de seguridad de la red del Departamento Administrativo del Consejo de Estado para la normalización y otros departamentos pertinentes del Consejo de Estado, sobre la base de sus responsabilidades individuales, organizar la formulación y revisión oportuna de las normas nacionales y de la industria relevantes para gestión de seguridad de la red, así como la seguridad de los productos de red, servicios y operaciones.

El Estado apoya a las empresas a participar en la formulación de normas nacionales y de la industria de seguridad de la red, y anima a las empresas a formular normas empresariales que sean más estrictas que las normas nacionales o de la industria.

Artículo 14: El Consejo de Estado y los gobiernos de las provincias, regiones autónomas y municipios gobernados de las personas harán integralmente planes; ampliar su entrada; apoyar a las industrias de tecnología de seguridad de red clave y programas; red de apoyo a la investigación de tecnología de seguridad y el desarrollo, aplicación y divulgación; proteger los derechos de propiedad intelectual de las redes de tecnología protector; instituciones de investigación y desarrollo de apoyo, instituciones de educación superior y las empresas para que participen en programas de innovación de tecnología de seguridad de red del Estado.

Artículo 15: Todos los niveles "de los gobiernos de las personas y sus departamentos competentes deberán organizar y llevar a cabo la publicidad de seguridad de red regular y la educación, y orientar y estimular las

unidades pertinentes en hacer publicidad de seguridad de red y el trabajo de educación también.

Los medios de comunicación deberán conducta dirigida publicidad seguridad de la red y la educación dirigida a la opinión pública.

Artículo 16: El Estado apoya a las empresas e instituciones de educación o de formación, como las instituciones de educación superior y centros de formación profesional, la realización de la educación relacionada con la seguridad de la red y la formación, y emplea varios métodos para cultivar el talento en tecnologías de seguridad de red, y promueve la interacción de la tecnología de seguridad de la red profesionales.

Capítulo III: Red De Operaciones De Seguridad

Sección 1: Disposiciones Generales

Artículo 17: El Estado implementa un sistema de protección de la seguridad de red en niveles Los operadores de red deberán cumplir los deberes siguientes de protección de seguridad de acuerdo a las exigencias del sistema de protección de seguridad de la red por niveles, para asegurar la red evita interferencias, daños o visitas no autorizadas, y para protegerse contra fugas de datos de red, robo o falsificación:

1. Formular sistemas de gestión de la seguridad interna y normas de funcionamiento, determinar las personas responsables de la seguridad de la red, y poner en marcha la red la responsabilidad de protección de seguridad;
2. Adoptar las medidas tecnológicas para prevenir los virus informáticos, ataques de red, intrusiones de red y otras acciones que pongan en peligro la seguridad de la red;
3. Adoptar las medidas tecnológicas para el registro y el seguimiento del estado de las operaciones de la red, y para el seguimiento y los incidentes de seguridad de la red de grabación, y conservar los registros de la red de acuerdo a las regulaciones;
4. Adoptar medidas como la clasificación de datos, copias de seguridad de datos importantes, y el cifrado;
5. Otras obligaciones previstas por la ley o los reglamentos administrativos.
Se proveerán las medidas específicas para la protección por niveles de seguridad de red para el Consejo de Estado.

Artículo 18: los productos y servicios de red deberán cumplir con las normas nacionales y relevantes de la industria. Los proveedores de productos y servicios de red no debe instalar programas maliciosos; donde sus productos y servicios tienen funciones la recopilación de información de los usuarios, ella se expresará a los usuarios y su consentimiento obtenido; cuando se descubre que sus productos o servicios de red tienen riesgos tales como

fallas de seguridad o fugas, informarán de inmediato a los usuarios y adoptar medidas correctivas.

Los proveedores de productos y servicios proporcionarán mantenimiento de la seguridad de sus productos y servicios de red; y no debe terminar proporcionando mantenimiento de la seguridad durante el período de tiempo establecido o el período acordado con los clientes.

Artículo 19: equipos de red crítico y productos especializados de seguridad de red se ajustará a los requisitos obligatorios de las normas nacionales y relevantes de la industria, y ser de seguridad certificada por un establecimiento calificado o cumplen con los requisitos de una inspección de seguridad, antes de ser vendidos. La administración nacional ciberespacio, junto con los departamentos pertinentes del Consejo de Estado, formular y liberan un catálogo de equipos de red críticos y productos especializados de seguridad de red, y fomentar el reconocimiento recíproco de las certificaciones de seguridad y resultados de las inspecciones de seguridad para evitar las certificaciones e inspecciones duplicadas.

Artículo 20: Los operadores de redes de manipulación de acceso a redes y servicios de registro de dominio para los usuarios, manejo de acceso a la red telefónica fija o móvil, o que proporcionan a los usuarios con servicios de publicación de la información, se requiere que los usuarios a proporcionar información verdadera identidad al firmar acuerdos con los usuarios o confirmar prestación de servicios. Cuando los usuarios no ofrecen verdadera identificar la información, los operadores de red no deben prestarles los servicios pertinentes.

El Estado apoya la investigación y desarrollo de tecnologías de confirmación de identidad electrónica segura y conveniente, promover la aceptación recíproca entre diferentes tecnologías de confirmación electrónicos identificar, y su uso común.

Artículo 21: operadores de red deberán elaborar planes de respuesta de emergencia para incidentes de seguridad de red, abordando rápidamente las fugas del sistema, virus informáticos, intrusiones en la red, ataques de red y otros riesgos de seguridad, la red; y cuando se producen incidentes de seguridad de red, inmediatamente iniciar el plan de respuesta de emergencia, adoptar las correspondientes medidas correctivas, e informar a los departamentos competentes de conformidad con las disposiciones pertinentes.

Artículo 22: Las personas u organizaciones no deben participar en las intrusiones de red o interferir con otras redes de funcionamiento ordinario, el robo de datos de la red u otras actividades perjudiciales para la seguridad de la red; que no deben proporcionar cualquiera de las herramientas o

métodos para hacer intrusiones en la red, lo que interfiere con el funcionamiento normal de las redes o robo de datos de la red u otras actividades perjudiciales para la seguridad de la red; no deben prestar asistencia, como soporte técnico, publicidad / promoción o apoyo financiero, etc.

Artículo 23: Para las necesidades de la seguridad nacional y la investigación penal, los órganos de investigación podrá solicitar a los operadores de red proporcionan soporte tecnológico nescesary y asistencia de conformidad con las leyes y reglamentos.

Artículo 24: El Estado apoya la cooperación entre los operadores de redes en áreas como la recopilación, análisis, presentación de informes y responsding a la red de información de seguridad, aumentando la capacidad de salvaguardia de seguridad de los operadores de red.

Organizaciones industriales pertinentes deberán establecer normas de protección de la seguridad de red robusta y mecanismos de coordinación para los sitios web de su propia industria, fortalecer su análisis y evaluación de la seguridad de la red, y en un plazo de tiempo determinado se comprometerán alertas de riesgo para los miembros, y deberá apoyar y coordinar las respuestas de los miembros a los riesgos.

Sección 2: Operaciones De Seguridad De Información De Infraestructuras Críticas

Artículo 25: El Estado implementa protecciones claves para las redes de información básicos que prestan servicios tales como la correspondencia pública y la radio y la difusión de la televisión; sistemas de información importantes para las industrias importantes como la energía, el transporte, la conservación del agua, y las finanzas, y las áreas de servicio público como los servicios públicos de electricidad, agua y gas, servicio médico y el saneamiento y la seguridad social; redes y asuntos gubernamentales militares redes para los órganos del Estado en el ámbito de la ciudad subdistricted y por encima; y las redes y los sistemas de propiedad o gestionados por los proveedores de servicios de red con un número masivo de los usuarios (en adelante "infraestructuras críticas de información". Las medidas para el establecimiento de medidas de seguridad para la infraestructura de información crítica se establecerán por el Consejo de Estado.

Artículo 26: departamentos del Consejo de Estado como para las comunicaciones, la radio y la televisión, la energía, el transporte, la conservación del agua, y las finanzas y otros departamentos pertinentes del Consejo de Estado (en lo sucesivo, los servicios encargados de la protección

de información crítica infraestructuras de los esfuerzos de protección de seguridad) , son individualmente responsables de orientar y supervisar el trabajo operativo de protección de seguridad para la infraestructura de información crítica, de acuerdo con las responsabilidades establecidas por el Consejo de Estado.

Artículo 27: La construcción de la infraestructura de información se asegurará de que tiene propiedades para el apoyo a la estabilidad de los negocios y operaciones de sostenimiento, y asegura que se planifican, establecen y utilizan simultáneamente medidas técnicas de seguridad.

Artículo 28: Salvo lo dispuesto en el artículo 17 de esta Ley, los operadores de infraestructuras críticas de información deberán realizar las siguientes funciones de protección de la seguridad:

1. Puesta en funcionamiento las instituciones y las personas responsables de la gestión de seguridad de gestión de seguridad especializados, y llevar a cabo los controles de seguridad en el fondo las personas responsables y personal en posiciones críticas;
2. Llevar a cabo periódicamente la educación red de seguridad, la capacitación técnica y la evaluación de las habilidades de los empleados;
3. Realizar copias de seguridad de desastres de los sistemas y bases de datos importantes;
4. Formular planes de respuesta de emergencia para incidentes de seguridad de la red, y organizar periódicamente simulacros;
5. Otras obligaciones previstas por la ley o los reglamentos administrativos.

Artículo 29: los operadores de infraestructura de información de productos de red de compra clave y servicios deberán firmar un acuerdo de confidencialidad con el proveedor de seguridad, aclarando los deberes y responsabilidades de seguridad y confidencialidad.

Artículo 30:. Operadores de infraestructura de información clave productos y servicios que pueden influir en la seguridad nacional deberán pasar por una inspección de seguridad organizado por la administración nacional ciberespacio y los departamentos pertinentes del Consejo de Estado de la red de compra de las medidas específicas se proporcionan por separado por el Consejo de Estado.

Artículo 31: información operadores de infraestructuras críticas deberá almacenar información personal de los ciudadanos, y otros datos importantes reunido y producido durante las operaciones, en el territorio continental de la República Popular de China; donde debido a los requerimientos del negocio que es verdaderamente necesario almacenar fuera de la parte continental o proporcionar a personas u organizaciones fuera de la parte continental, deberán seguir las medidas formuladas

conjuntamente por la administración nacional ciberespacio y los departamentos pertinentes del Consejo de Estado para llevar a cabo una seguridad evaluación. Cuando las leyes o regulaciones administrativas dispongan lo contrario, siga estas disposiciones.

Artículo 32: Al menos una vez al año, los operadores de infraestructuras críticas de información llevará a cabo una inspección y evaluación de su seguridad y de los riesgos que podrían existe ya sea redes personalmente, o por medio de retención de una institución especializada; y presentar un informe de seguridad de red de las circunstancias de la inspección y evaluación, así como las medidas de mejora adoptadas, que se enviará al departamento pertinente responsable de los esfuerzos críticos de protección de la seguridad de infraestructura de información.

Artículo 33:. La administración nacional ciberespacio coordinará los departamentos pertinentes en su conjunto, el establecimiento de un mecanismo de coordinación con respecto a la protección de la seguridad de la infraestructura de información crítica, las siguientes medidas podrán adoptarse:

1. Con respecto a las pruebas de inspección aleatoria de los riesgos de seguridad a la infraestructura de información crítica, [pueden] proponer medidas de mejora, y cuando sea necesario para ello podrán designar instituciones de inspección y detección de especialistas para llevar a cabo las pruebas y la evaluación de los riesgos de seguridad;
2. Periódicamente organizan operadores de infraestructuras de información crítica para llevar a cabo simulacros de seguridad de la red de emergencia, aumentando el nivel y la coordinación de las respuestas respuestas de infraestructura de información crítica para la red incidentes de seguridad.
3. Promover la seguridad de la red intercambio de información entre los departamentos pertinentes, los operadores de infraestructuras críticas de información, las instituciones de servicios de seguridad de redes e instituciones de investigación pertinentes información.
4. Proporcionar apoyo técnico y asistencia para la gestión de emergencias de seguridad de red y la recuperación y así sucesivamente...

Capítulo IV: Red De Información Sobre Seguridad

Artículo 34: Los operadores de red deberán establecer y sistemas completos de protección de la información del usuario, el fortalecimiento de la protección de los usuarios de la información personal, la privacidad y secretos comerciales.

Artículo 35: Red de operadores de recolección y uso de información personal de los ciudadanos deberán respetar los principios de legalidad, decencia y la

necesidad, indicando explícitamente los objetivos, medios y el alcance de la recopilación o el uso de la información, y la obtención del consentimiento de la persona cuyos datos se reunieron.
Los operadores de red no deben recopilar información personal de los ciudadanos sin relación con los servicios que prestan; no debe violar las disposiciones de las leyes, reglamentos administrativos o los acuerdos bilaterales para recoger o utilizar información personal de los ciudadanos; y se ajustará a las disposiciones de las leyes, reglamentos administrativos o acuerdos con los usuarios para procesar la información personal de los ciudadanos que han ahorrado.

Los operadores de red a recoger o utilizar información personal de los ciudadanos tienen que revelar sus reglas para su recopilación y uso.

Artículo 36: Red de los operadores deben mantener la información personal de los ciudadanos que recogen estrictamente confidencial y no deben revelar, deformar o dañarlo, y no deben vender o ilegalmente ofrecer a los demás.

Los operadores de redes deberán adoptar las medidas tecnológicas y de otra índole necesarias para garantizar la seguridad de la información personal de los ciudadanos y evitar que la información personal de los ciudadanos a los que reúne fugas, daños o pérdidas. Cuando, daños o pérdidas se producen circunstancias de la fuga de información, o podrían ocurrir, correctivas medidas se tomarán de inmediato, los usuarios que puedan verse afectados serán informados, y los informes se harán a los servicios competentes de conformidad con la normativa.

Artículo 37: En caso de ciudadanos descubren los operadores de redes han violado las disposiciones de las leyes, reglamentos administrativos o los acuerdos bilaterales para recoger o utilizar sus datos personales, que tienen el derecho de solicitar a los operadores de redes de borrar su información personal; donde el descubrimiento de que la información personal recopilada o almacenada por los operadores de red tiene errores, tienen el derecho de solicitar a los operadores de redes hacen correcciones.

Artículo 38: Persona u organización no deben robar o utilizar otros métodos ilegales para adquirir los ciudadanos la información personal, y no deben vender o ilegalmente ofrecer a otros con los ciudadanos información personal.

Artículo 39: Departamentos con funciones de supervisión de la seguridad de la red y gestión de conformidad con la ley, debe mantener la información personal de los ciudadanos, la información privada y secretos comerciales que aprender de en el desempeño de sus funciones estrictamente

confidencial y no debe tener fugas, vender o ilegalmente proporcionarla a otros.

Artículo 40: Red operadores deberán fortalecer la gestión de la información publicada por los usuarios, y donde descubrir la información que la ley o los reglamentos administrativos prohíbe la publicación o transmisión de, deberán cesar de inmediato la transmisión de esa información, emplear medidas de tratamiento como eliminarla, evitar que el la información se propague, guardar los registros pertinentes, e informar a los departamentos cometent pertinentes.

Artículo 41: La información electrónica enviada por los peticionarios de información electrónica y software de aplicaciones proporcionadas por los proveedores de software de aplicación no debe instalar programas maliciosos, y no debe contener información que las leyes y reglamentos administrativos prohíben la publicación o transmisión de.

La información digital proveedores de servicios de distribución y proveedores de servicios de descargas de software de aplicación se perfom tareas de administración de seguridad; y donde el descubrimiento de que los distribuidores digitales de información o proveedores de software de aplicaciones tienen una conducta prevista en el párrafo anterior, deberá detener la prestación del servicio y emplear medidas de disposición como la eliminación, el almacenamiento de los registros pertinentes e informar a los departamentos competentes.

Artículo 42: Red de operadores establecerán red queja seguridad de la información y presentación de informes, se da publicidad a la información como los métodos para la presentación de quejas o reportes, y rápidamente la aceptación y el manejo de quejas y los informes pertinentes a la red de seguridad de la información.

Artículo 43: La administración nacional ciberespacio y los departamentos pertinentes realizan red de supervisión y administración de la seguridad responsabilidades; y donde el descubrimiento de la información de la liberación o la transmisión de lo que está prohibido por las leyes de los reglamentos administrativos, deberán solicitar la transmisión operadores de redes de parada, emplear medidas de disposición como la eliminación y almacenar los registros pertinentes; para la información descrita anteriormente que viene de fuera del continente República Popular de China, lo notificarán a la organización pertinente adoptar medidas tecnológicas y otras medidas necesarias para bloquear la transmisión de información.

Capítulo V: El Monitoreo, Alertas Tempranas, Y La Respuesta De Emergencia

Artículo 44: El Estado establece los sistemas de alerta y de boletines de información rápida y de control de seguridad de la red y la administración nacional ciberespacio hará la coordinación general de los departamentos pertinentes para fortalecer la recopilación, el análisis y los esfuerzos de informes para la información de seguridad de la red, y realizar la liberación unificada de supervisión de la seguridad de la red e información de alerta temprana, de acuerdo con las regulaciones.

Artículo 45: Departamentos responsables de las actividades de protección de seguridad de infraestructura de información crítica debe establecer y completar esa industria o un control de seguridad de red de ese campo y la alerta temprana y la información de los sistemas de información, e informar la supervisión de seguridad de la red y la información de alerta temprana, de acuerdo con las regulaciones.

Artículo 46: La administración nacional ciberespacio coordina los departamentos pertinentes 'establecer y terminación de los mecanismos de los esfuerzos de respuesta de emergencia de seguridad de red, formular incidentes de seguridad los planes de respuesta de emergencia de la red, y periodicly organizar simulacros.

Departamentos responsables de las actividades de protección de seguridad de infraestructura de información crítica deberá formular esa industria o los planes de respuesta de emergencia a incidentes de seguridad de red de ese campo, y periódicamente organizar simulacros.

Los planes de respuesta de emergencia a incidentes de seguridad de red deberán clasificar los incidentes de seguridad de la red sobre la base de factores tales como el grado de amenaza después de que ocurra el incidente y el alcance del impacto, y proporcionar medidas de manejo de emergencia correspondiente.

Artículo 47: Cuando los incidentes de seguridad de la red están a punto de ocurrir o donde su probabilidad de ocurrencia aumenta, los departamentos pertinentes de los gobiernos populares a nivel de condado y de nivel superior, de acuerdo con su autoridad, y los procedimientos establecidos por las leyes, las leyes y reglamentos administrativos y Estado reglamentos del Consejo, emitir información de advertencia correspondiente a su rango, y de acuerdo a las características del incidente que está a punto de suceder o daño que pueda resultar, esos departamentos podrán adoptar las siguientes medidas:

1. Exigir que los departamentos competentes, las instituciones y el personal se reúnen con prontitud y reportar información relevante y fortalecer la vigilancia de la ocurrencia de incidentes de seguridad de la red y el desarrollo de la situación;
2. Organice los departamentos competentes, instituciones y personal especializado para llevar a cabo el análisis y la evaluación de los datos de los incidentes de seguridad de la red, y predecir la probabilidad de ocurrencia, el alcance del impacto y nivel de daño de los incidentes;
3. anunciar públicamente la información de predicción y los resultados de los análisis / evaluaciones que conciernen al público;
4. De acuerdo con las regulaciones anunciar públicamente advertencias como para dañar a los incidentes de seguridad de la red, y anunciar medidas de prevención y reducción de daños.

Artículo 48: En la ocurrencia de incidentes de seguridad de la red, los departamentos pertinentes de los gobiernos de la gente a nivel de condado o supra se iniciará inmediatamente el plan de respuesta de emergencia a incidentes de seguridad de la red, realizar una evaluación y valoración del incidente de seguridad de red, solicitar que los operadores de redes adoptan tecnológica y otras medidas necesarias, eliminar los riesgos de seguridad potentional, evitar la amenaza de la creciente, y liberan rápidamente medidas de precaución pertinentes para el público.

Artículo 49: En caso de emergencias repentinas o accidentes de seguridad de producción se producen como consecuencia de los incidentes de seguridad de la red, se tramitará de conformidad con lo dispuesto en las leyes pertinentes, tales como la "Ley de Respuesta a Emergencias de la República Popular China" y la "seguridad de Producción Ley de la República Popular de China".

Artículo 50: Para cumplir con la necesidad de proteger la seguridad nacional y el orden público social y responder a incidentes importantes de seguridad social, el Consejo de Estado, o de los gobiernos de las provincias, regiones autónomas y municipios con la aprobación por el Consejo de Estado, podrá adoptar las medidas temporales relativas comunicaciones de red en ciertas regiones, como la restricción de la misma.

Capítulo VI Responsabilidad Legal

Artículo 51: En caso de los operadores de red no realizan tareas de protección de seguridad de red previstas en los artículos 17 y 21 de esta ley, los servicios competentes podrán pedir correcciones y dar advertencias; donde correcciones se denieguen o que conduce a la puesta en peligro de la seguridad de red u otras consecuencias, dar una multa de entre 10.000 y 100.000 RMB; y multar al personal de gestión responsables directos entre 5.000 y 50.000 RMB.

Cuando la información crítica operadores de infraestructuras no realizan funciones de protección de la seguridad de la red previstos en los artículos 27-29 y 32 de esta ley, los servicios competentes podrán pedir correcciones y dar advertencias; donde correcciones se denieguen o que conduce a la puesta en peligro de la seguridad de red u otras consecuencias, dar una multa de 100.000 yuanes y 1.000.000; y multar al personal de gestión responsables directos entre 10.000 y 100.000 RMB.

Artículo 52: En caso de proveedores de productos y servicios de red, transmisión de información electrónica y proveedores de software de aplicación presentan cualquiera de las siguientes conductas en violación de esta ley, las pertinentes órdenes de departamentos competentes correcciones y da advertencias; donde las correcciones se negaron o causa puesta en peligro de la seguridad de red u otras consecuencias, una multa de entre 50.000 y 500.000 RMB se da; y las personas que están directamente a cargo son multados entre 10.000 y 100.000 RMB.

1. Instalación de programas maliciosos;
2. Sus productos o servicios tienen funciones que recogen la información del usuario, sin expresar esto a los usuarios y obtener su consentimiento;
3. Existen riesgos tales como fallas de seguridad o vulnerabilidades en sus productos o servicios, pero no informan de inmediato al usuario y para tomar las medidas correctivas;
4. terminación no autorizada para el mantenimiento de la seguridad de sus productos y servicios.

Artículo 53: Los operadores de redes que violen esta ley al no obligar a los usuarios a proporcionar información veraz identidad o la prestación de servicios correspondientes a los usuarios que no proporcionan información sobre la identidad verdadera, se ordenó hacer correcciones por el departamento competente; donde correcciones se denieguen o las circunstancias son graves, se le da una multa de 50.000 yuanes y 500.000, y el departamento competente podrá ordenar la suspensión temporal de las operaciones, una suspensión de negocio para las correcciones, el cierre de los sitios web, la revocación de las operaciones correspondientes permisos o cancelación de licencias comerciales; las personas que están directamente a cargo y otros miembros del personal directamente responsables son multados entre 10.000 y 100.000 RMB.

Artículo 54: Los operadores de redes que violen esta ley en infringir las protecciones y derechos de información personal de los ciudadanos, se ordenó hacer correcciones por el departamento competente y puede, advertencias, ya sea de forma independiente o al mismo tiempo, ser dadas, la confiscación de las ganancias ilícitas y / o una multa de entre 1 a 10 veces el importe de las ganancias ilícitas, y donde no hay ganancias ilícitas, multa

de hasta 500.000 RMB; donde las circunstancias son graves, se le da una multa de 50.000 yuanes y 500.000, y el departamento competente podrá ordenar la suspensión temporal de las operaciones, una suspensión de negocio para las correcciones, el cierre de los sitios web, la revocación de los permisos de operaciones relevantes, o cancelación de licencias comerciales; las personas que están directamente a cargo y otros miembros del personal directamente responsables son multados entre 10.000 y 100.000 RMB.

Dónde violaciónes de esta ley en el robo o el uso de otros medios ilegales para obtener, vender de manera ilegal proporcionar a otros con la información personal de los ciudadanos, no constituyen un delito, los órganos de seguridad pública confiscar las ganancias ilícitas y dar una multa de entre 1 y 10 veces la cantidad de las ganancias ilícitas, y donde no hay ganancias ilícitas, dar una multa de hasta 500.000 RMB.

Artículo 55: En caso de información crítica operadores de infraestructuras violan el artículo 30 de esta ley mediante el uso de productos de red o servicios que no han tenido inspecciones de seguridad o no aprobar las inspecciones de seguridad, los departamentos competentes ordenan el uso de parar, y le dan una multa por la cantidad de 1 a 10 veces el precio de compra; las personas que están directamente a cargo y otros miembros del personal directamente responsables son multados entre 10.000 y 100.000 RMB.

Artículo 56: En caso de información crítica operadores de infraestructuras violan esta ley mediante el almacenamiento de datos de la red fuera del territorio continental, o proporcionar datos de la red a las personas u organizaciones fuera del territorio continental sin pasar por una evaluación de la seguridad, las órdenes de departamentos pertinentes correcciones competentes, da advertencias, confisca ganancias ilícitas, da multas de entre 50.000 y 500.000 RMB, y puede ordenar una suspensión temporal de las operaciones, una suspensión de negocio para las correcciones, el cierre de los sitios web, la revocación de los permisos de operaciones relevantes, o cancelación de licencias comerciales; las personas que están directamente a cargo y otros miembros del personal directamente responsables son multados entre 10.000 y 100.000 RMB.

Artículo 57: En caso de los operadores de redes violan esta ley al no detener la transmisión de la información que las leyes de regulaciones administrativas prohíben la publicación o transmisión de, al no emplear medidas de disposición como la eliminación o el fracaso de conservar los registros pertinentes, las órdenes de departamentos pertinentes correcciones competentes , da advertencias y confisca ganancias ilegales; donde correcciones se denieguen o circunstancias son graves, se dan multas de entre 50.000 RMB y 500.000, y una suspensión temporal de

las operaciones, una suspensión de negocio para las correcciones, el cierre de los sitios web, la revocación de los permisos de operaciones relevantes, o cancelación de licencias de negocios pueden ser ordenada; las personas que están directamente a cargo y otros miembros del personal directamente responsables son multados entre 10.000 y 100.000 RMB.

Cuando los proveedores de servicios de información electrónica y de software de aplicación los proveedores de servicios de descarga, no han realizado sus obligaciones de seguridad en virtud de esta Ley, el castigo que de conformidad con lo dispuesto en el párrafo anterior.

Artículo 58: La publicación o la transmisión de la información que las leyes o reglamentos administrativos prohíben la publicación o transmisión de, es castigado de acuerdo con las disposiciones de las leyes y reglamentos administrativos.

Artículo 59: Los operadores de red en violación de las disposiciones de esta ley, en los siguientes casos, deberá corregir su violación en virtud de órdenes del departamento responsable pertinente; si se niegan a corregir o las circunstancias son graves, serán multados no menos de 50.000 RMB y no más de 500.000 RMB; personal responsable que son directamente responsables y demás personal directamente responsables serán multados no menos de 10.000 RMB y no más de RMB 100.000:

1. El no reportar los riesgos de seguridad de red o incidentes de seguridad de red a las autoridades pertinentes;
2. La negativa u obstrucción de los departamentos competentes en la supervisión legal y la inspección;
3. La negativa a proporcionar el apoyo y la asistencia necesaria.

Artículo 60: Cuando hay una conducta pone en peligro la seguridad netowrk en violación del artículo 22 de esta ley que no constituye un delito, o donde hay otra conducta que viola las disposiciones de esta ley que constituye una violación administrativa de seguridad pública, se dará sanciones administrativas de seguridad pública de conformidad con la ley.

Artículo 61: En caso de operadores de redes de asuntos gubernamentales de órganos del Estado no realizan funciones de protección de la seguridad de la red según lo prescrito por la presente ley, el órgano en el nivel superior o departamento competente ordenará la corrección; sanciones se dan a los gestores responsables directos y otro personal directamente responsables.

Artículo 62: Cuando el personal de los departamentos que llevan de supervisión y gestión de la seguridad de la red deberes, descuidan sus deberes, abusar de su oficina, o distorsionan la ley para beneficio personal,

sin constituir un delito, las sanciones administrativas se dan de conformidad con la ley.

Artículo 63: En caso de violaciónes de las disposiciones de esta ley causa daño a los demás, la responsabilidad civil está a cargo de conformidad con la ley.

Artículo 64: En caso de violaciónes de esta Ley constituyen un delito, perseguir la responsabilidad penal de conformidad con la ley.

Capítulo VII: Disposiciones Complementarias

Artículo 65: Para esta ley, los siguientes términos tienen estos significados:
1. "Redes" se refiere a las redes y sistemas compuestos por ordenadores u otros terminales de información y material relacionado que seguir ciertas reglas y procedimientos para la recopilación de información, almacenamiento, transmisión, intercambio y procesamiento.

2. "La seguridad de la red" se refiere a la adopción de medidas necesarias para prevenir ataques, invasión, perturbación, que socavan y uso ilegal de redes, así como los accidentes inesperados; haciendo que las redes para estar en un estado de funcionamiento estable y fiable, así como salvaguardar la integridad, confidencialidad y capacidad de uso de la red de almacenamiento de información, transmisión y procesamiento.

3. "Los operadores de red" se refiere a los propietarios y administradores de redes, así como los proveedores de servicios de red utilizando redes de propiedad o administrados por otros de prestación de servicios relacionados; incluyendo operadores básicos de telecomunicaciones, proveedores de servicios de información de la red, los principales operadores de sistemas de información y así sucesivamente.

4. "Los datos de la red" se refiere a todo tipo de datos electrónicos recogidos, almacenados, transmitidos, procesados, y produce a través de las redes
"Datos personales del ciudadano" 5. refiere a un datos personales - como el nombre de un ciudadano, fecha de nacimiento, número de tarjeta de identificación, los datos biométricos personales, profesión, domicilio, o número de teléfono - grabada electrónicamente o por otros medios, como así como todos los otros tipos de datos desde la que se puede determinar la identidad de un ciudadano, ya sea por sí mismo o en combinación con otros datos.

Artículo 66: protección de la seguridad de Operaciones para el almacenamiento y redes de procesamiento que implique una información secreto de Estado, además de seguir esta ley, deberá respetar también las leyes, reglamentos administrativos y normas sobre clasificación.

Artículo 67: la red militar y de protección de seguridad de la información las medidas son formulados por la Comisión Militar Central.

Artículo 68: La presente ley entrará en vigor el XXXXX.

网络安全法（草案）

By CLT On July 6, 2015.

来源：
http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm

2015年6月，**第十二届全国人大常委会第十五次会**议初次审议了《中华人民共和国网络安全法（草案）》。现将《中华人民共和国网络安全法（草案）》在中国人大网公布，向社会公开征求意见。**社会公众可以直接登**录中国人大网（www.npc.gov.cn）**提出意**见，也可以将意见寄送全国人大常委会法制工作委员会（北京市西城区前门西大街1**号**，邮编：100805。

中华人民共和国网络安全法（草案）

第一章　总　　则

第一条　为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条　**在中**华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条　**国家**坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设，鼓励网络技术创新和应用，建立健全网络安全保障体系，提高网络安全保护能力。

第四条　**国家倡**导诚实守信、健康文明的网络行为，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第五条　**国家**积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间。

第六条　**国家网信部**门负责统筹协调网络安全工作和相关监督管理工作。 **国**务院工业和信息化、公安部门和其他有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责按照国家有关规定确定。

第七条　**建**设、运营网络或者通过网络提供服务，应当依照法律、法规的规定和国家标准、行业标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第八条　**网**络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员依法加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第九条　**国家保**护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、**便利的网**络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法和法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、宣扬恐怖主义和极端主义、宣扬民族仇恨和民族歧视、传播淫秽色情信息、侮辱诽谤他人、扰乱社会秩序、损害公共利益、侵害他人知识产权和其他合法权益等活动。

第十条　**任何个人和**组织都有权对危害网络安全的行为向网信、工业和信息化、公安等部门举报。 **收到**举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

第二章　网络安全战略、规划与促进

第十一条　**国家制定网**络安全战略，明确保障网络安全的基本要求和主要目标，提出完善网络安全保障体系、提高网络安全保护能力、促进网络安全技术和产业发展、推进全社会共同参与维护网络安全的政策措施等。

第十二条　**国**务院通信、广播电视、能源、交通、水利、金融等行业的主管部门和国务院其他有关部门应当依据国家网络安全战略，编制关系国家安全、国计民生的重点行业、重要领域的网络安全规划，并组织实施。

第十三条　**国家建立和完善网**络安全标准体系。 **国**务院标准化行政主管部门和国务院其他有关部门根据各**自的**职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业参与网络安全国家标准、行业标准的制定，并鼓励企业制定严于国家标准、行业标准的企业标准。

第十四条　**国**务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发、应用和推广，保护网络技术知识产权，支持科研机构、高等院校和企业参与国家网络安全技术创新项目。

第十五条　**各**级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做**好网**络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第十六条　**国家支持企**业和高等院校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全技术人才，促进网络安全技术人才交流。

第三章　网络运行安**全**

第一节　一般规**定**

第十七条　**国家**实行网络安全等级保护制度。 **网**络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）**制定内部安全管理制度和操作**规程，确定网络安全负责人，落实网络安全保护责任；

（二）**采取防范**计算机病毒和网络攻击、网络入侵等危害网络安全行为的技术措施；

（三）**采取**记录、跟踪网络运行状态，监测、记录网络安全事件的技术措施，并按照规定留存网络日志；

（四）**采取数据分**类、重要数据备份和加密等措施；

（五）**法律、行政法**规规定的其他义务。

网络安全等级保护的具体办法由国务院规定。

第十八条　**网**络产品、服务应当符合相关国家标准、行业标准。 **网**络产品、服务的提供者不得设置恶意程序；其产品、服务具有收集用户信息功能的，应当向用户明示并取得同意；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当及时向用户告知并采取补救措施。**网**络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期间内，不得终止提供安全维护。

第十九条　**网**络关键设备和网络安全专用产品应当按照相关国家标准、行业标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售。 **国家网信部**门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十条　**网**络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。 **用**户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证技术之间的互认、通用。

第二十一条　**网**络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络入侵、网络攻击等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规**定向有关主管部**门报告。

第二十二条　**任何个人和**组织不得从事入侵他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供从事入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全活动的工具和制作方法；不得为他人实施危害网络安全的活动提供技术支持、广告推广、支付结算等帮助。

第二十三条　为国家安全和侦查犯罪的需要，侦查机关依照法律规定，可以要求网络运营者提供必要的支持与协助。

第二十四条　**国家支持网**络运营者之间开展网络安全信息收集、分析、通报和应急处置等方面的合作，提高网络运营者的安全保障能力。**有关行**业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第二节　关键信息基础设施的运行安**全**

第二十五条　**国家**对提供公共通信、广播电视传输等服务的基础信息网络，能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统，军事网络，设区的市级以上国家机关等政务网络，用户数量众多的网络服务提供者所有或者管理的网络和系统（以下称关键信息基础设施），实行重点保护。**关**键信息基础设施安全保护办法由国务院制定。

第二十六条　**国**务院通信、广播电视、能源、交通、水利、金融等行业的主管部门和国务院其他有关部门（以下称负责关键信息基础设施安全保护工作的部门）按照国务院规定的职责，分别负责指导和监督关键信息基础设施运行安全保护工作。

第二十七条　**建**设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第二十八条　除本法第十七条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期组织演练；

（五）法律、行政法规规定的其他义务。

第二十九条　关键信息基础设施的运营者采购网络产品和服务，应当与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十条　关键信息基础设施的运营者采购网络产品或者服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的安全审查。具体办法由国务院规定。

第三十一条　关键信息基础设施的运营者应当在中华人民共和国境内存储在运营中收集和产生的公民个人信息等重要数据；因业务需要，确需在境外存储或者向境外的组织或者个人提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。法律、行政法规另有规定的从其规定。

第三十二条　关键信息基础设施的运营者应当自行或者委托专业机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并对检测评估情况及采取的改进措施提出网络安全报告，报送相关负责关键信息基础设施安全保护工作的部门。

第三十三条　国家网信部门应当统筹协调有关部门，建立协作机制。对关键信息基础设施的安全保护可以采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托专业检验检测机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高关键信息基础设施应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施运营者以及网络安全服务机构、有关研究机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与恢复等，提供技术支持与协助。

第四章　网络信息安全

第三十四条　网络运营者应当建立健全用户信息保护制度，加强对用户个人信息、隐私和商业秘密的保护。

第三十五条　网络运营者收集、使用公民个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的公民个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用公民个人信息，并应当依照法律、行政法规的规定或者与用户的约定，处理其保存的公民个人信息。

网络运营者收集、使用公民个人信息，应当公开其收集、使用规则。

第三十六条　网络运营者对其收集的公民个人信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

网络运营者应当采取技术措施和其他必要措施，确保公民个人信息安全，防止其收集的公民个人信息泄露、毁损、丢失。 在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，告知可能受到影响的用户，并按照规定向有关主管部门报告。

第三十七条　公民发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。

第三十八条　任何个人和组织不得窃取或者以其他非法方式获取公民个人信息，不得出售或者非法向他人提供公民个人信息。

第三十九条　依法负有网络安全监督管理职责的部门，必须对在履行职责中知悉的公民个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十条　网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十一条　电子信息发送者发送的电子信息，应用软件提供者提供的应用软件不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，发现电子信息发送者、应用软件提供者有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十二条　网络运营者应当建立网络信息安全投诉、举报平台，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

第四十三条　国家网信部门和有关部门依法履行网络安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断信息传播。

第五章　监测预警与应急处置

第四十四条　国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第四十五条　负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第四十六条　国家网信部门协调有关部门建立健全网络安全应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第四十七条　网络安全事件即将发生或者发生的可能性增大时，县级以上人民政府有关部门应当依照有关法律、行政法规和国务院规定的权限和程序，发布相应级别的预警信息，并**根据即将**发生的事件的特点和可能造成的危害，采取下列措施：

（一）**要求有关部**门、机构和人员及时收集、报告有关信息，加强对网络安全事件发生、发展情况的监测；

（二）组织有关部门、机构和专业人员，对网络安全事件信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）**向社会**发布与公众有关的预测信息和分析评估结果；

（四）**按照**规定向社会发布可能受到网络安全事件危害的警告，发布避免、减轻危害的措施。

第四十八条　发生网络安全事件，县级以上人民政府有关部门应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第四十九条　**因网**络安全事件，发生突发事件或者安全生产事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律的规定处置。

第五十条　**因**维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，国务院或者省、自治区、直辖市人民政府经国务院批准，可以在部分地区对网络通信采取限制等临时措施。

第六章　法律责**任**

第五十一条　**网**络运营者不履行本法第十七条、第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款；对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第二十七条至第二十九条、第三十二条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一

百万元以下罚款；对直接负责的主管人员处一万元以上十万元以下罚款。

第五十二条 网络产品、服务的提供者，电子信息发送者，应用软件提供者违反本法规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款；对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）其产品、服务具有收集用户信息功能，未向用户明示并取得同意的；

（三）对其产品、服务存在的安全缺陷、漏洞等风险未及时向用户告知并采取补救措施的；

（四）擅自终止为其产品、服务提供安全维护的。

第五十三条 网络运营者违反本法规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、撤销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第五十四条 网络运营者违反本法规定，侵害公民个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处五十万元以下罚款；情节严重的，可以责令暂停相关业务、停业整顿、关闭网站、撤销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法规定，窃取或者以其他方式非法获取、出售或者非法向他人提供公民个人信息，尚不构成犯罪的，由公安机关没收违法所得，并

处违法所得一倍以上十倍以下罚款，没有违法所得的，处五十万元以下罚款。

第五十五条　关键信息基础设施的运营者违反本法第三十条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第五十六条　关键信息基础设施的运营者违反本法规定，在境外存储网络数据，或者未经安全评估向境外的组织或者个人提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、撤销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第五十七条　网络运营者违反本法规定，对法律、行政法规禁止发布或者传输的信息**未停止**传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、撤销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处二万元以上二十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，未履行本法规定的安全义务的，依照前款规定处罚。

第五十八条　发布或者传输法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第五十九条　网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款；对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）**未将网**络安全风险、网络安全事件向有关主管部门报告的；

（二）**拒**绝、阻碍有关部门依法实施的监督检查的；

（三）**拒不提供必要的支持与**协助的。

第六十条　有本法第二十二条规定的危害网络安全的行为，尚不构成犯罪的，或者有其他违反本法规定的行为，构成违反治安管理行为的，依法给予治安管理处罚。

第六十一条　国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第六十二条　依法负有网络安全监督管理职责的部门的工作人员，玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予行政处分。

第六十三条　违反本法规定，给他人造成损害的，依法承担民事责任。

第六十四条　违反本法规定，构成犯罪的，依法追究刑事责任。

第七章　附　　则

第六十五条　本法下列用语的含义:

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的网络和系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络存储、传输、处理信息的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者以及利用他人所有或者管理的网络提供相关服务的网络服务提供者，包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）公民个人信息，是指以电子或者其他方式记录的公民的姓名、出生日期、身份证件号码、个人生物识别信息、职业、住址、电话号码等个人身份信息，以及其他能够单独或者与其他信息结合能够识别公民个人身份的各种信息。

第六十六条　存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第六十七条 军事网络和信息安全保护办法，由中央军事委员会制定。

第六十八条 本法自　　年　月　日起施行。

Cybersecurity Law (Draft)

By CLT On July 6, 2015 ·

Source：

http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm

The 15th meeting of the Standing Committee of the 12th National People's Congress performed initial review of this "People's Republic of China Cybersecurity Law (Draft)" in June 2014. The " People's Republic of China Cybersecurity Law (Draft)" is hereby released to the public on the Chinese National People's Congress website for collection of public comments. The public can directly log in to the NPC website ((www.npc.gov.cn)) and provide comments; and may also mail comments to the National People's Congress Legal Work Committee, (Beijing, Xicheng District, Qianmen West Road #1, 100805) [in Chinese: **北京市西城区前**门西大街1**号**，邮编：100805]

People's Republic of China Cybersecurity Law (draft)

Chapter 1: General Provisions

Article 1: This law is formulated so as to ensure network security, to preserve cyberspace sovereignty, national security and societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social informatization.

Article 2: This law applies with respect to the construction, operation, maintenance and usage of networks, as well as the supervision and management of networks within the mainland territory of the People's Republic of China.

Article 3: The State persists in equally stressing network security and informatization development, and abides by the directives of positive use, scientific development, management according to the law, and ensuring security; and advances the construction of network infrastructure, encouraging innovation and application of network technology, establishing and completing network security guarantee systems, and raising the capacity to protect network security.

Article 4: The State advocates sincere, honest, healthy and civilized network conduct, adopting measures to raise the entire society's network security awareness and level, and forming a good environment for the entire society to jointly participate in advancing network security.

Article 5: The State actively launches international exchange and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, attacking cybercrime and illegality, and other such areas; promoting the construction of a peaceful, secure, open and cooperative cyberspace.

Article 6: The national cyberspace administration is responsible for comprehensively planning and coordinating network security efforts and related supervision and management efforts. The State Council Ministry of Industry and Information Technology, and public security, as well as other relevant departments, are responsible for network security protection, supervision and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law, relevant laws and administrative regulations.

Network security protection, supervision and management duties for relevant departments in people's governments at the county level or above will be determined by relevant State regulations.

Article 7: The construction and operation of networks or provision of services through networks shall be in accordance with the provisions of laws and regulations and the mandatory requirements of State or industry standards; adopting technical measures and other necessary measures to protect network security and operational stability, effectively responding to network security incidents, preventing cyber crimes, and safeguarding the integrity, secrecy and usability of online data.

Article 8: Relevant network trade organizations are to, according to their Articles of Association, strengthen industry self-discipline, formulate behavioural network security norms, guide their members in strengthening network security protection according to the law, raise the protection levels of network security, and stimulate the healthy development of the industry.

Article 9: The State protects the rights of citizens, legal persons and other organizations to use networks according to the law; it promotes widespread network access, raises the level of network services, it provides secure and convenient network services to society, and guarantees the lawful, orderly and free circulation of network information.

Any person and organization shall, when using the network, abide by the the Constitution and laws, observe public order and respect social morality, they must not endanger network security, and must not use the network to engage in activities harming national security, propagating of terrorism and extremism, inciting ethnic hatred and ethnic discrimination, dissemination of obscene and sexual information, slandering or defame others, upsetting social order, harming the public interest, infringing of other persons' intellectual property or other lawful rights and interests.

Article 10: All individuals and organizations have the right to report conduct endangering network security to departments such as for network information, industry and information technology, public security. Departments receiving reports shall promptly process them in accordance with law; where these do not fall within the responsibility of that department, it shall promptly transfer the matter to the department empowered to handle it.

Chapter II: Network Security Strategy, Planning And Promotion

Article 11: The State formulates a network security strategy, clarifying the basic requirements and main objectives of guaranteeing network security, putting forward and improving network security safeguard systems, raising the capacity for network security protection, stimulating the development of network security technology and industry, and moving forward policy measures to preserve network security with participation from the entire society, and so forth.

Article 12: The State Council departments for telecommunications, radio and television, energy, transportation, water conservancy, finance and other such industries and other relevant State Council departments shall, on the basis of the national network security strategy, compile network security plans concerning national security, major industries for the national economy and the people's livelihood, and important fields, and organize their implementation.

Article 13: The State establishes and improves a system of network security standards. The State Council administrative department for standardization and other relevant State Council departments, on the basis of their individual responsibilities, organise the formulation and timely revision of relevant national and industry standards for network security management as well as the security of network products, services and operations.

The State supports enterprises to participate in the formulation of national and industry standards for network security, and encourages enterprises to formulate enterprise standards that are stricter than the national or industry standards.

Article 14:The State Council and people's governments of provinces, autonomous regions and directly-governed municipalities shall make comprehensively plans; expand their input; support key network security technology industries and programs; support network security technology research and development, application and popularization; protect the intellectual property rights of technology protecting networks; support research and development institutions, higher education institutions, and enterprises to participate in State network security technology innovation programs.

Article 15: All levels' of people's governments and their relevant departments shall organise and carry out regular network security publicity and education, and guide and stimulate relevant units in doing network security publicity and education work well.

The mass media shall conduct targeted network security publicity and education aimed at the public.

Article 16: The State supports enterprises and education or training institutions such as higher learning institutions and vocational schools, carrying out network security-related education and training, and employs multiple methods to cultivate talent in network security technologies, and promotes interaction of network security technology professionals.

Chapter III: Network Operations Security

Section 1: General Provisions

Article 17: The State implements a tiered network security protection system. Network operators shall fulfill the following security protection duties according to the requirements of the tiered network security protection system, to ensure the network avoids interference, damage or unauthorised visits, and to guard against network data leaks, theft or falsification:

1. Formulate internal security management systems and operating rules, determine persons responsible for network security, and implement network security protection responsibility;

2. Adopt technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering network security;

3. Adopt technological measures for recording and tracking the status of network operations, and for monitoring and recording network security incidents, and preserve network logs according to regulations;

4. Adopt measures such as data classification, back-up of important data, and encryption;

5. Other obligations as provided by law or administrative regulations.

Specific measures for tiered network security protection shall be provided for by the State Council.

Article 18: Network products and services shall comply with the relevant national and industry standards. Providers of network products and services must not install malicious programs; where their products and services have functions gathering users' information, this shall be expressed to users and their consent obtained; when it is discovered that their network products or services have risks such as security flaws or leaks, they shall promptly inform users and adopt remedial measures.

Providers of network products and services shall provide security maintenance for their products and services; and must not terminate providing security maintenance during the set time period or period agreed on with clients.

Article 19: Critical network equipment and specialized network security products shall follow the compulsory requirements of relevant national and industry standards, and be safety certified by a qualified establishment or meet the requirements of a security inspection, before being sold. The national cyberspace administration together with the relevant departments of the State Council, formulate and release a catalog of critical network equipment and specialized network security products, and promote reciprocal recognition of safety certifications and security inspection results to avoid duplicative certifications and inspections.

Article 20: Network operators handling network access and domain registration services for users, handling stationary or mobile phone network access, or providing users with information publication services, shall require users to provide real identity information when signing agreements with users or confirming provision of services. Where users do not provide real identify information, network operators must not provide them with relevant services.

The State supports research and development of secure and convenient electronic identity confirmation technologies, promoting reciprocal acceptance among different electronic identify confirmation technologies, and their common use.

Article 21:network operators shall formulate emergency response plans for network security incidents, promptly addressing system leaks, computer viruses, network intrusions, network attacks and other such network security risks; and when network security incidents occur, immediately initiate the emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Article 22:Individuals or organisation must not engage in network intrusions, or interfering with other networks ordinary functioning, theft of network data or any other activities harmful to network security ; they must not provide either the tools or methods for making network intrusions, interfering with the ordinary functioning of networks or theft of network data or other activities harmful to network security ; they must not provide assistance such as technical support, advertising/promotion, or financial support etc.

Article 23: For the needs of national security and criminal investigation, investigating organs may request network operators provide nescesary technological support and assistance in accordance with laws and regulations.

Article 24: The State supports cooperation between network operators in areas such as gathering, analyzing, reporting and responsding to network security information, increasing the security safeguard capacity of network operators.

Relevant industry organisations shall establish robust network security protection rules and coordination mechanisms for their own industry's websites, strengthen their analysis and evaluation of network security , and within a designated period of time shall undertake risk alerts for members, and shall support and coordinate members' responses to risks.

Section 2: Operations Security For Critical Information Infrastructure

Article 25:The State implements key protections for basic information networks providing services such as public correspondence and radio and television broadcast; important information systems for important industries such as energy, transportation, water conservation, and finance, and public service areas such as electricity, water and gas utilities, medical and sanitation service and social security; military networks and government affairs networks for state organs at the subdistricted city level and above; and networks and systems owned or managed by network service providers with massive numbers of users (hereinafter "critical information infrastructure". Measures for establishing security safeguards for critical information infrastructure shall be enacted by the State Council.

Article 26:State Council departments such as for communications, radio and television, energy, transportation, water conservancy, and finance and other relevant departments of the State Council (hereinafter referred to as departments responsible for the protection of critical information infrastructures security protection efforts), are individually responsible for guiding and supervising operational security protection work for critical information infrastructure, in accordance with responsibilities provided by the State Council.

Article 27: Construction of information infrastructure shall ensure that it has properties for supporting business stability and sustaining operations, and ensures that technical security measures are planned, established and used concurrently.

Article 28: Except as provided in article 17 of this Law, critical information infrastructure operators shall perform the following security protection duties:

1. Set up specialized security management institutions and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;

2. Periodically conduct network security education, technical training and skills assessment for employees;

3. Conduct disaster backups of important systems and databases;

4. Formulate emergency response plans for network security incidents, and periodically organize drills;

5. Other obligations as provided by law or administrative regulations.

Article 29: Key information infrastructure operators purchasing network products and services shall sign a security confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality.

Article 30: Key information infrastructure operators purchasing network products and services that might influence national security shall go through a security inspection organized by the national cyberspace administration and relevant departments of the State Council. Specific measures are provided separately by the State Council.

Article 31: Critical information infrastructure operators shall store citizens' personal information, and other important data gathered and produced during operations, within the mainland territory of the People's Republic of China ; where due to business requirements it is truly necessary to store it outside the mainland or provide it to individuals or organizations outside the mainland, they shall follow the measures jointly formulated by the national cyberspace administration and the relevant departments of the State Council to conduct a security assessment. Where laws or administrative regulations otherwise provide, follow those provisions.

Article 32:At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks security and risks that might exists either personally, or through retaining a specialized institution; and submit a network security report on the circumstances of the inspection and assessment as well as improvement measures taken, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.

Article 33: The national cyberspace administration shall coordinate relevant departments as a whole, establishing a coordination mechanism. With respect to the security protection of critical information infrastructure, the following measures may be adopted:

1. With respect to random inspection testing of security risks to critical information infrastructure, [they may] propose measures for improvement, and when necessary to do so may appoint specialist inspection and detection institutions to undertake testing and evaluation for security risks;

2. Periodically organize critical information infrastructure operators to conduct emergency network security drills, increasing the level and coordination of responses critical information infrastructure responses to network security incidents.

3. Promote network security information sharing among relevant departments, critical information infrastructure operators, network security services institutions and relevant research institutions.

4. Provide technical support and assistance for network security emergency management and recovery and so forth..

Chapter IV: Network Information Security

Article 34: Network operators shall establish and complete user information protection systems, strengthening protection of users personal information, privacy, and commercial secrets.

Article 35: Network operators collecting and using citizens' personal information shall abide by principles of legality, propriety and necessity, explicitly stating the purposes, means and scope for collecting or using information, and obtaining the consent of the person whose data is gathered.

Network operators must not gather citizens' personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or bilateral agreements to gather or use citizens' personal information; and shall follow the provisions of laws, administrative regulations or agreements with users to process citizens' personal information they have saved.

Network operators collecting or using citizens' personal information shall disclose their rules for its collection and use.

Article 36: Network operators must keep citizens' personal information they collect strictly confidential and must not disclose, distort or damage it, and must not sell or illegally provide it to others.

Network operators shall adopt technological measures and other necessary to ensure the security of citizen's personal information, and prevent the citizens' personal information it gathers from leaking, damage or loss. When circumstances of information leaks, damage or loss occur, or might occur, remedial measures shall be immediately taken, users who might be affected shall be informed, and reports shall be made to the competent departments in accordance with regulations.

Article 37: Where citizens discover network operators have violated the provisions of laws, administrative regulations or bilateral agreements to gather or use their personal information, they have the right to request the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to request the network operators make corrections.

Article 38: Individual or organization must not steal or use other illegal methods to acquire citizens' personal information, and must not sell or unlawfully provide others with citizens' personal information.

Article 39: Departments with duties of network safety supervision and management in accordance with law, must keep citizens' personal information, private information and commercial secrets they learn of in

performing their duties strictly confidential, and must not leak, sell, or unlawfully provide it to others.

Article 40: Network operators shall strengthen management of information published by users, and where discovering information that the law or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ treatment measures such as deleting it, prevent the information from spreading, save relevant records, and report to the relevant cometent departments.

Article 41: Electronic information sent by electronic information submitters and application software provided by application software providers must not install malicious programs, and must not contain information that laws and administrative regulations prohibit the publication or transmission of.

Digital information distribution service providers and application software download service providers shall perfom security administration duties; and where discovering that digital information distributors or application software providers have conduct provided for in the preceding paragraph, shall stop the provision of service and employ disposition measures such as deletion, storing relevant records and reporting to the relevant competent departments.

Article 42: Network operators shall establish network information security complaint and reporting system, publicly disclosing information such as the methods for making complaints or reports, and promptly accepting and handling complaints and reports relevant to network information security.

Article 43:The national cyberspace administration and relevant departments perform network security supervision and administration responsibilities; and where discovering information the release or transmission of which is prohibited by laws of administrative regulations, shall request the network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside mainland People's Republic of China, they shall notify the relevant organization to adopt technological measures and other necessary measures to block the transmission of information.

Chapter V: Monitoring, Early Warnings, And Emergency Response

Article 44: The State establishes network security monitoring and early warning and information bulletin systems. The national cyberspace administration shall do overall coordination of relevant departments to strengthen collection, analysis and reporting efforts for network security information, and perform unified release of network security monitoring and early warning information in accordance with regulations.

Article 45: Departments responsible for critical information infrastructure security protection efforts shall establish and complete that industry or that field's network security monitoring and early warning and information reporting systems, and report network security monitoring and early warning information in accordance with regulations.

Article 46: The national cyberspace administration coordinates relevant departments' establish and completion of mechanisms for network security emergency response efforts, formulate network security incident emergency response plans, and periodicly organize drills.

Departments responsible for critical information infrastructure security protection efforts shall formulate that industry or that field's network security incident emergency response plans, and periodically organize drills.

Network security incident emergency response plans shall rank network security incidents on the basis of factors such as the degree of threat after the incident occurs and the scope of impact, and provide corresponding emergency response handling measures.

Article 47: When network security incidents are about to occur or where their probability of occurring increases, relevant departments of county-level people's governments and above shall, according to their authority, and the procedures prescribed by relevant laws, administrative laws and regulations and State Council regulations, issue warning information corresponding to their rank, and according to the characteristics of the incident which is about to happen or harm which is likely to result, those departments may adopt the following measures:

1. Require that competent departments, institutions and personnel promptly gather and report relevant information and strengthen monitoring of the occurrence of network security incidents and the development of the situation;

2. Organise competent departments, institutions and specialist personnel to undertake analysis and evaluation of data from the network security incidents, and predict the incidents' likelihood of occurrence, scope of impact and level of harm;

3. Publicly announce the prediction information and the results of analyses/evaluations which concern the public;

4. According to regulations publicly announce warnings as to harm from the network security incidents, and announce measures for avoidance and reduction of harm.

Article 48: On occurrence of network security incidents, relevant departments of people's governments at the county level or above shall

immediately initiate the network security incident emergency response plan, conduct an evaluation and assessment of the network security incident, request that network operators adopt technological and other necessary measures, remove potentional security risks, prevent the threat from growing, and promptly release cautionary measures relevant to the public.

Article 49: Where sudden emergencies or production safety accidents occur as a result of network security incidents, it shall be handled in accordance with the provisions of relevant laws such as the "Emergency Response Law of the People's Republic of China" and the "Production Safety Law of the People's Republic of China".

Article 50: To fulfill the need to protect national security and social public order, and respond to major social security incidents, the State Council, or the governments of provinces, autonomous regions and municipalities with approval by the State Council, may take temporary measures regarding network communications in certain regions, such as restricting it.

Chapter VI Legal Responsibility

Article 51: Where network operators do not perform network security protection duties provided for in articles 17 and 21 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of network security or other such consequences, give a fine of between RMB 10,000 and 100,000; and fine the directly responsible management personnel between RMB 5,000 and 50,000.

Where critical information infrastructure operators do not perform network security protection duties provided for in articles 27-29 and 32 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of network security or other such consequences, give a fine of between RMB 100,000 and 1, 000,000; and fine the directly responsible management personnel between RMB 10,000 and 100,000.

Article 52:Where providers of network products and services, electronic information transmission and application software providers exhibit any of the following conduct in violation of this law, the relevant competent department orders corrections and gives warnings; where corrections are refused or it causes endangerment of network security or other consequences, a fine of between RMB 50,000 and 500,000 is given; and the persons who are directly in charge are fined between RMB 10,000 and 100,000.

1. Installing malicious programs;

2. Their products or services have functions collecting user information, without expressing this to users and obtaining their consent;

3. Risks such as security flaws or vulnerabilities exist in their products or services, but do not promptly inform the user and to take remedial measures;

4. Unauthorized termination for the security maintenance of its products and services.

Article 53: Network operators violating this law in failing to require users to provide truthful identity information or providing relevant services to users who do not provide truthful identity information, are ordered to make corrections by the relevant competent department; where corrections are refused or the circumstances are serious, a fine of between RMB 50,000 and 500,000 is given, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Article 54: Network operators violating this law in infringing on the protections and rights of citizens' personal information, are ordered to make corrections by the relevant competent department and may ,either independently or concurrently, be given warnings, confiscation of unlawful gains, and/or fined between 1 to 10 times the amount of unlawful gains, and where there are no unlawful gains, fined up to RMB 500,000; where the circumstances are serious, a fine of between RMB 50,000 and 500,000 is given, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Where violations of this law in stealing or using other illegal means to obtain, sell of illegally provide others with citizens' personal information do not constitute a crime, the public security organs confiscate unlawful gains and give a fine of between 1 and 10 times the amount of unlawful gains, and where there are no unlawful gains, give a fine of up to RMB 500,000.

Article 55: Where critical information infrastructure operators violate article 30 of this law by using network products or services that have not had safety inspections or did not pass safety inspections, the relevant competent departments order the usage to stop, and give a fine in the amount of 1 to 10 times the purchase price; the persons who are directly in charge and

other directly responsible personnel are fined between RMB 10,000 and 100,000.

Article 56: Where critical information infrastructure operators violate this law by storing network data outside the mainland territory, or provide network data to individuals or organizations outside of the mainland territory without going through a security assessment, the relevant competent department orders corrections, gives warnings, confiscates unlawful gains, gives fines between RMB 50,000 and 500,000, and may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Article 57: Where network operators violate this law by failing to stop the transmission of information that laws of administrative regulations prohibit the publication or transmission of, failing to employ disposition measures such as deletion or failure to preserve relevant records, the relevant competent department orders corrections, gives warnings, and confiscates unlawful gains; where corrections are refused or circumstances are serious, fines between RMB 50,000 and 500,000 are given, and a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses may be ordered; persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Where electronic information services providers and application software download service providers, have not performed their security obligations under this Act, punishment i in accordance with the provisions of the preceding paragraph.

Article 58: Publication or transmission of information that laws or administrative regulations prohibit the publication or transmission of, is punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 59: Network operators in violation of the provisions of this law, in the following circumstances, shall correct their violation pursuant to orders of the relevant responsible department; if they refuse to correct or the circumstances are serious, they shall be fined not less than RMB 50,000 and not more than RMB 500,000; responsible personnel who are directly liable and other directly liable personnel shall be fined not less than RMB 10,000 and not more than RMB 100,000:

1. Failure to report network security risks or network security incidents to the relevant authorities;

2. Refusal or obstruction of the competent departments in their lawful supervision and inspection;

3. Refusal to provide necessary support and assistance.

Article 60: Where there is conduct endangering netowrk security in violation of article 22 of this law that does not constitute a crime, or where there is other conduct violating provisions of this law that constitutes a public security administrative violation, public security administrative sanctions are given in accordance with law.

Article 61: Where state organ government affairs network operators do not perform network security protection duties as prescribed by this law, the organ at the level above or relevant department will order corrections; sanctions are given to the managers directly responsible and other directly responsible personnel.

Article 62: Where personnel of departments bearing network safety supervision and management duties, neglect their duties, abuse their office, or distort the law for personal gain, without constituting a crime, administrative sanctions are given in accordance with law.

Article 63: Where violations of the provisions of this law cause harm to others, civil liability is borne in accordance with law.

Article 64: Where violations of this Law constitute a crime, pursue criminal responsibility in accordance with law.

Chapter VII: Supplementary Provisions

Article 65: For this law, the following terms have these meanings:

1. "Networks" refers to networks and systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing.

2. "Network safety" refers to taking necessary measures to prevent attacks, invasion, disturbance, undermining and unlawful use of networks, as well as unexpected accidents; causing the networks to be in a state of stable and reliable operation, as well as safeguarding the integrity, secrecy and usability of network information storage, transmission, and processing.

3. "Network operators" refers to the owners and administrators of networks, as well as network service providers using networks owned or administrated by others to provide related services; including basic telecommunications

operators, network information service providers, major information system operators and so on.

4. "Network data" refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks

5. "Citizen's personal data" refers to a personal data -- such as a citizen's name, birth date, identification card number, personal bio-metric data, profession, residence, or telephone number -- recorded electronically or by other means, as well as all other kinds of data from which a citizen's identity may be determined, either by itself or combined with other data.

Article 66: Operations security protection for storing and processing networks involving state secret information, in addition to following this law, shall also uphold laws, administrative regulations and rules on classification.

Article 67: Military network and information security protection measures are formulated by the Central Military Commission.

Article 68: This law shall take effect on XXXXX.