$ NcN 2k26



Quien soy

> SecOpsDev

> Formador, cuando me dejan
> Investigador en mis ratos libres
> Activista tecnológico
  - Soberanía tecnológica
  - Defensor de la privacidad
  - Cofundador de Hacklabs y M4H
> redmicelio.com





Censura







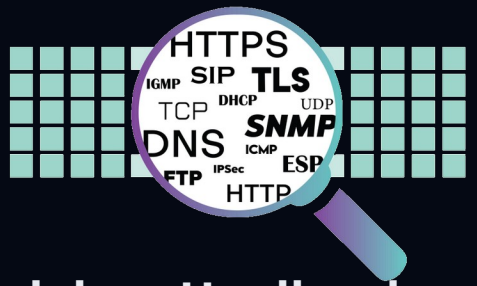
Cómo se censura

FW



IP, DNS ...

DPI



Clave-palabra, Huellas de protocolos

Corte de Internet



Gran Cortafuegos / GFW



TSPU

1º Distribuida
y
descentralizada



2º Distribuida
Y
centralizada

Cronología Legal

1995 SORM-1

> Sistema para actividades operativas de investigación.

> Herramienta física y tecnológica el "cómo" se intercepta

> Interceptación legal de comunicaciones



Cronología Legal

1995 SORM-1

1999 Rechazo control

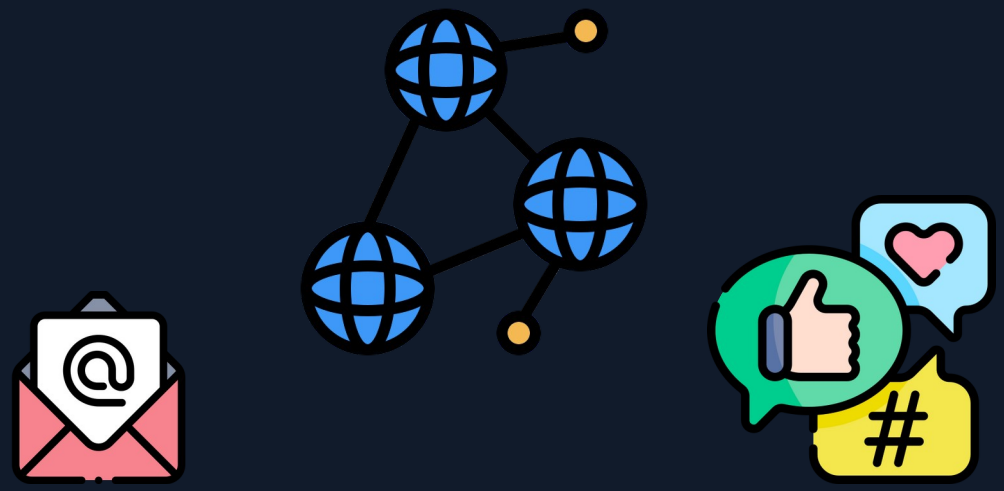
> Propuesta de control de Dominios e Ips



Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)

> Centrada en Internet



Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN

> **Roskomnadzor** o **RKN** (Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación)



Cronología Legal

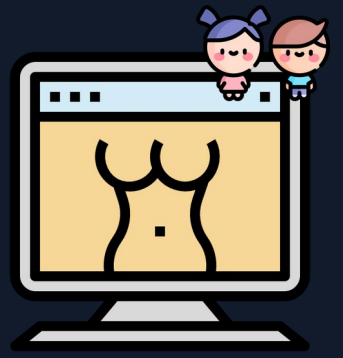
1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra

> Registro de sitios prohibidos. (gestionado por roskomnadzor)

> Pretesto proteger menores

> Los operadores bloqueaban por su cuenta







Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos

> Ley bloqueo extrajudicial
> Ley de blogueros





>3000 visitas día

Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3

> Recopilación de metadatos (hora , fecha, la ubicación, el remitente y los destinatarios de los mensajes y archivos multimedia

> Inspección profunda de paquetes (DPI), almacenamiento de datos largo plazo y filtrado avanzado por identificadores (IP, teléfono, IMEI o MAC)

Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea

> Tras la anexión de Crimea, se utilizó para censurar blogs de opositores como **Alekséi Navalny** y portales de noticias independientes



Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea
2016 Ley Yarovaya

> SORM es el "cómo" se intercepta, la ley Yarovaya es el mandato jurídico (el "qué" y "por cuánto tiempo" se debe guardar)

> Metadatos 3 años y Contenido 6 meses

>Los datos almacenados deben ponerse a disposición de las autoridades, **sin necesidad de una orden**.

> El FSB tiene acceso **sin cifrar** al correo electronico y las redes sociales

Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea
2016 Ley Yarovaya

> Se instaura el Sistema Automático Revizor (AS Revizor)



Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea
2016 Ley Yarovaya
2016 Plataformas extranjera bloqueadas

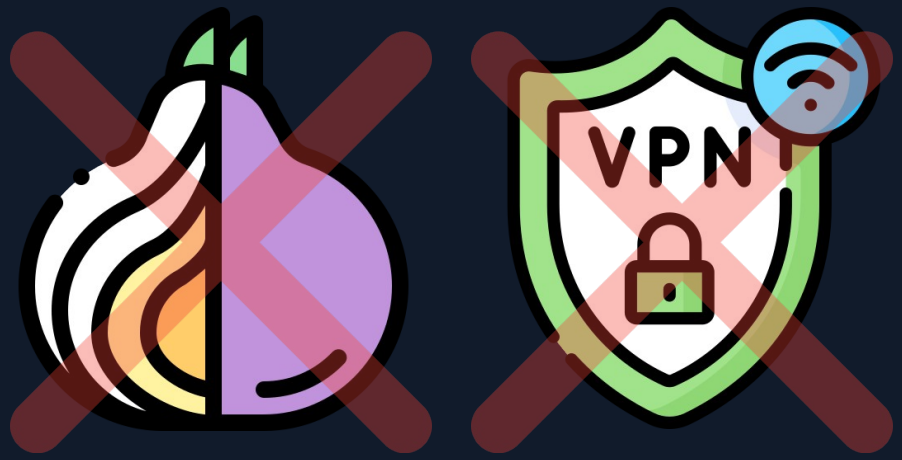
> LinkedIn fueron bloqueadas por negarse a almacenar los datos de ciudadanos rusos en servidores locales



Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea
2016 Ley Yarovaya
2016 Plataformas extranjera bloqueadas
2017 Ley sobre VPN y anonimizadores

> Prohibición de anonimizadores y VPN que no filtren la lista negra



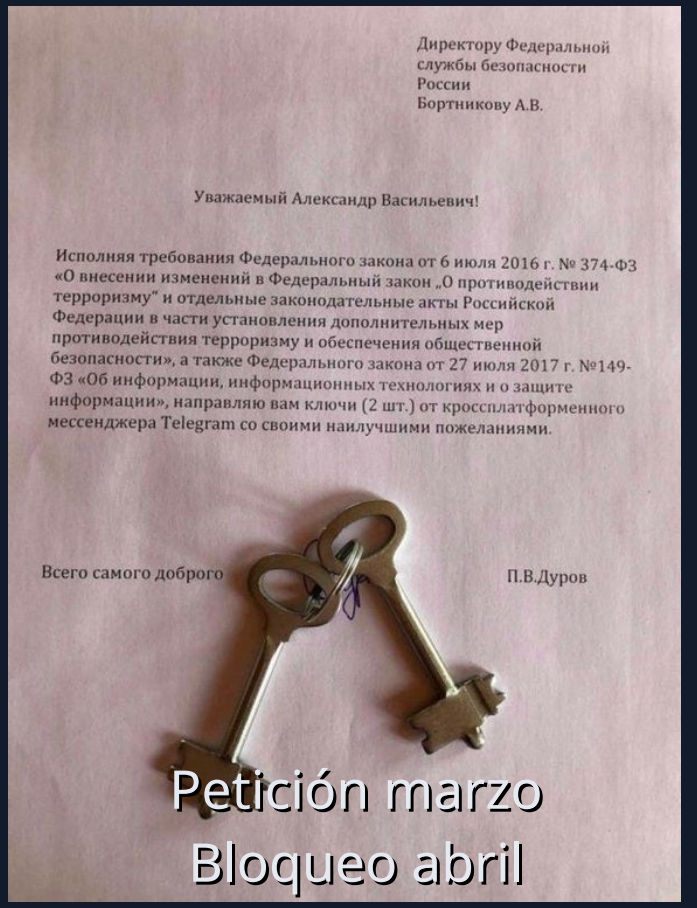
Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea
2016 Ley Yarovaya
2016 Plataformas extranjera bloqueadas
2017 Ley sobre VPN y anonimizadores
2018 Bloqueo telegram

> Los creadores de **telegram** se negaron a entregar las llaves de cifrado de los usuarios tras la petición de Roskomnadzor

Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea
2016 Ley Yarovaya
2016 Plataformas extranjera bloqueadas
2017 Ley sobre VPN y anonimizadores
2018 Bloqueo telegram



Cronología Legal

1995 SORM-1
1999 Rechazo control
2000 SORM-2 (1998)
2008 Roskomnadzor o RKN
2012 Ley de la lista negra
2013-2014 Bloqueos
2014 SORM-3
2014 Anexión de Crimea
2016 Ley Yarovaya
2016 Plataformas extranjera bloqueadas
2017 Ley sobre VPN y anonimizadores
2018 Bloqueo telegram

Pavel Durov

2024



Telegram entregará las direcciones IP y los números de teléfono de los usuarios a las autoridades

Cronología Legal

2019 Ley de internet (Runet) soberana

> 30 Actos normativos
> Equipamiento **único (TSPU)**
> Control de los IXP
> Lista de Cables transforenterizos
> Centralización de la censura
> Soberanía Tecnologica
> **DNS Nacional (NSDI)**
> Fin de la semilibertad de ISP

Dificultades analisis



> Solo se bloquean conexiones iniciadas desde Rusia

> Solo redes residenciales, centros de datos casi nada

> Dificultad por marcarse como objetivo del estado



Las "Cajas Negras" TSPU

TSPU; Medios Técnicos para Contrarrestar Amenazas

> Controlar, filtrar y ralentizar

> Desarrollados por empresas vinculadas al Estado

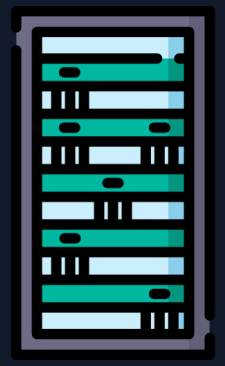
> Despliegue lo realiza RKN y FSB bajo llave

> El operador no tiene control, solo obligaciones

> Conectados in-line (en serie) en cada Operador

TSPU - Hardware

Equipos de computo

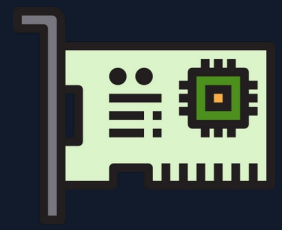


HUAWEI

intel

SUPERMICRO

Equipos de redes

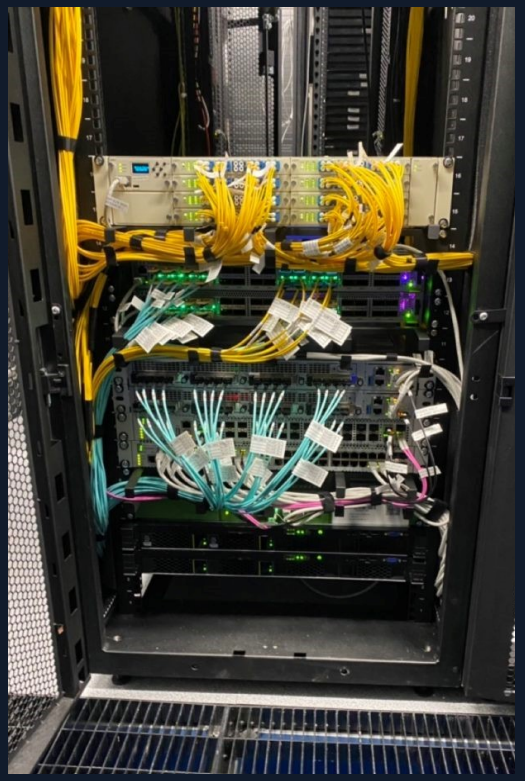


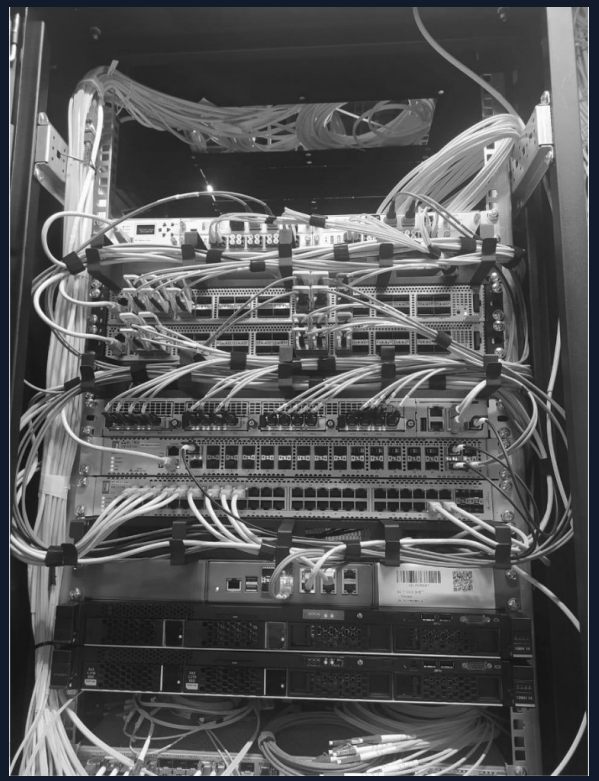
Mellanox TECHNOLOGIES

intel

TSPU - Hardware

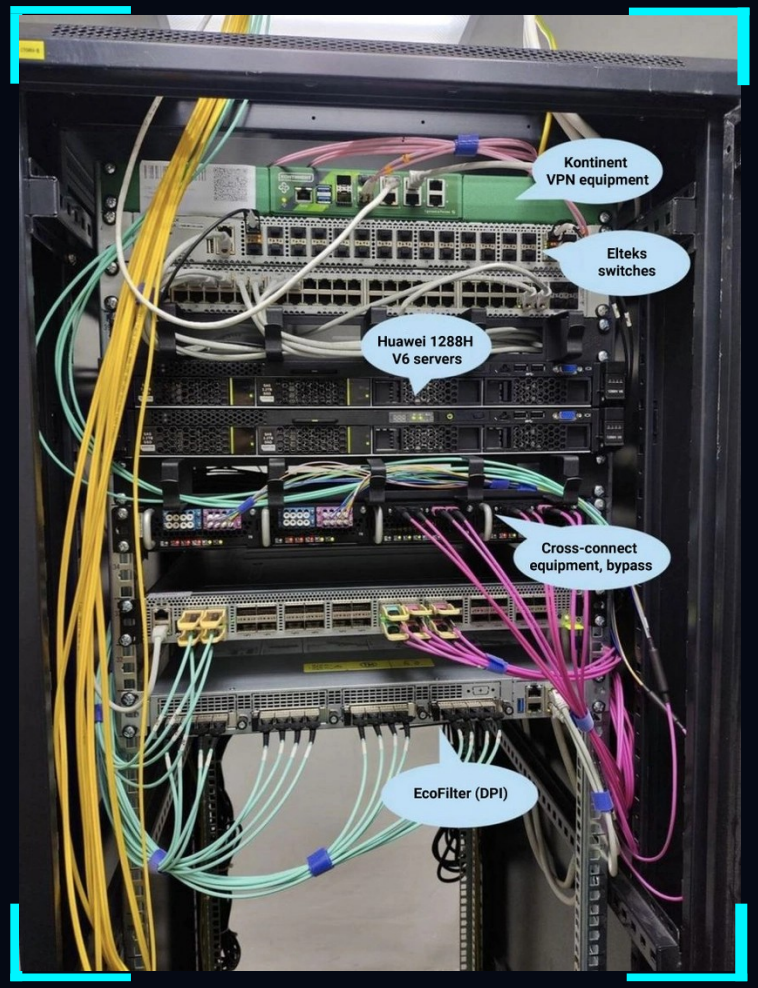






Fuente: Archivo personal de Mikhail Klimarev

TSPU - Hardware



> **EcoDPI** es el módulo DPI para analizar, clasificar y restringir el tráfico

> **Servidores**; cómputo y gestión donde corren los sistemas de control, recolección y registro

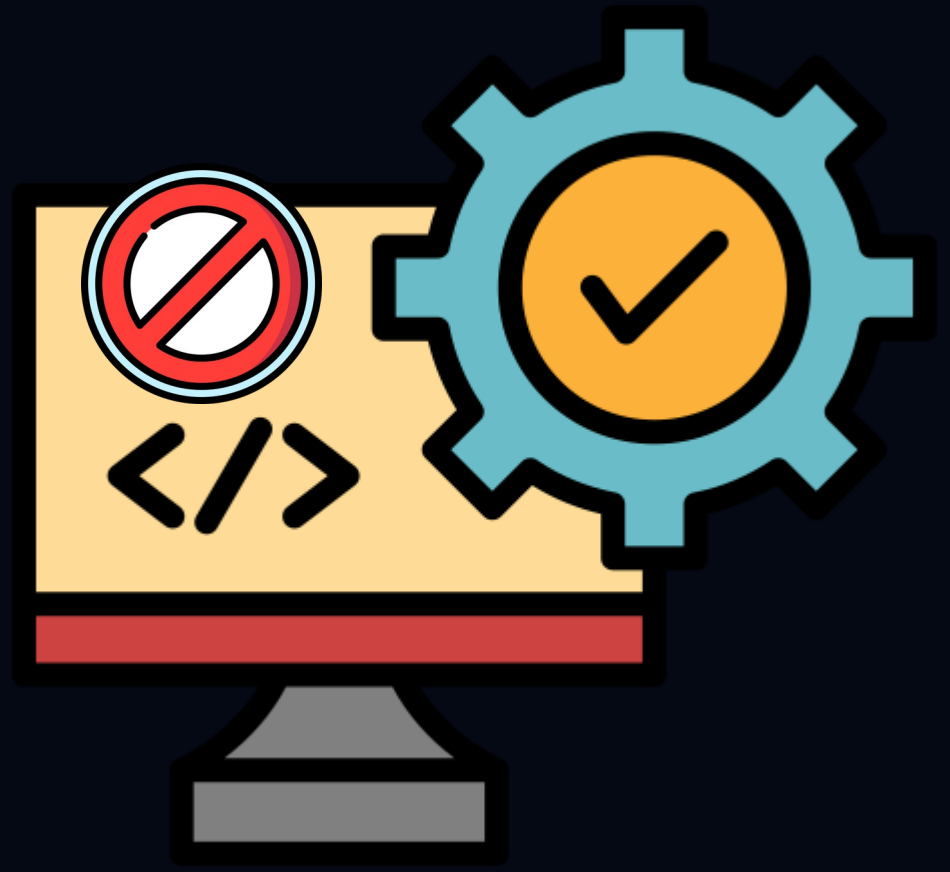
> **Switch de red**

> **Switch de Bypass**

> **Módulos ópticos**

> **Kontinent;** Software/Hardware de cifrado

Funcionamiento del TSPU



> Cuando un usuario intenta acceder, el TSPU mira primero el DNS

> Si usa DNS cifrado, el TSPU lee el campo SNI

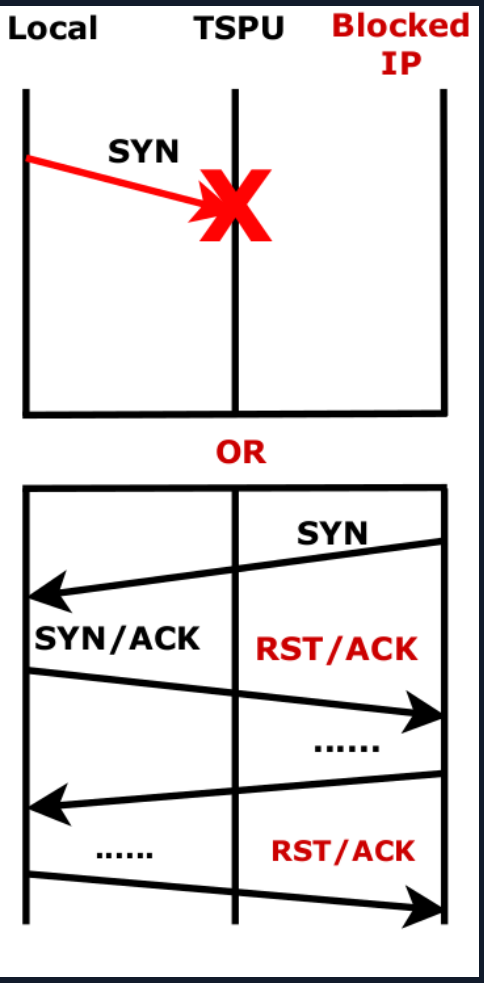
Bloqueos – IP Based

> Solo IP, no evalua ni puerto ni el contenido

> Si un cliente ruso contacta con la IP bloqueada, sus paquetes salientes se descartan

> Si la IP bloqueada inicia la conexión hacia un servidor en Rusia, la petición pasa, pero la respuesta pierde su contenido (RST/ACK)

> Los pings ICMP también se descartan



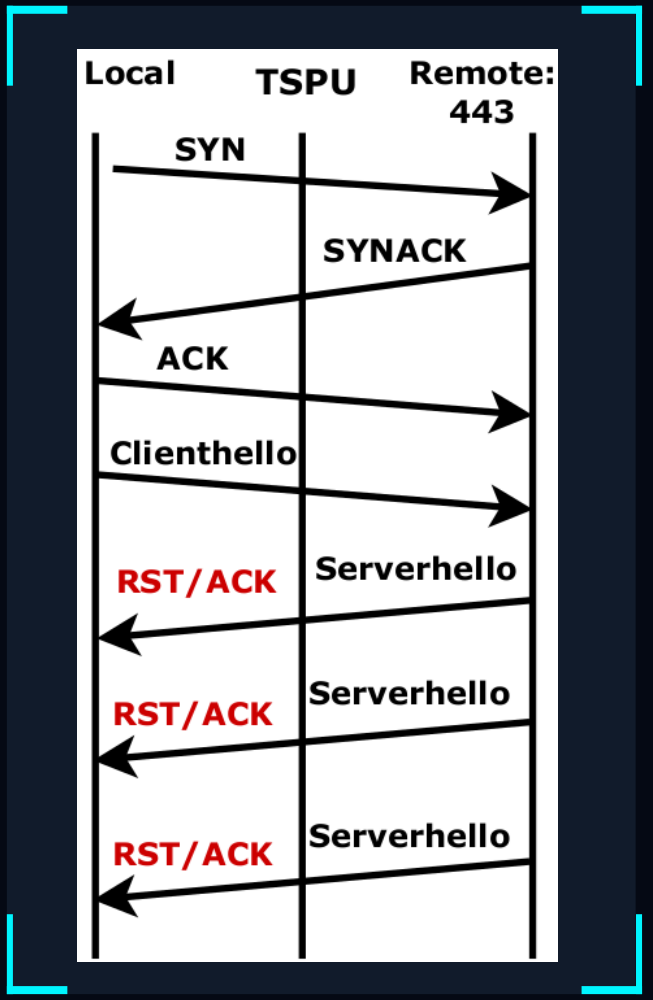
Bloqueos - SNI Based I

> Tras ver el ClientHello, modifica los paquetes que vienen del servidor remoto hacia el cliente ruso. Les recorta el contenido y cambia las banderas TCP a RST/ACK

> TTL y números de secuencia no se tocan

> El cliente cree que el servidor cerró la conexión. Solo actúa en dirección descendente

> Duración del estado: unos 75 segundos

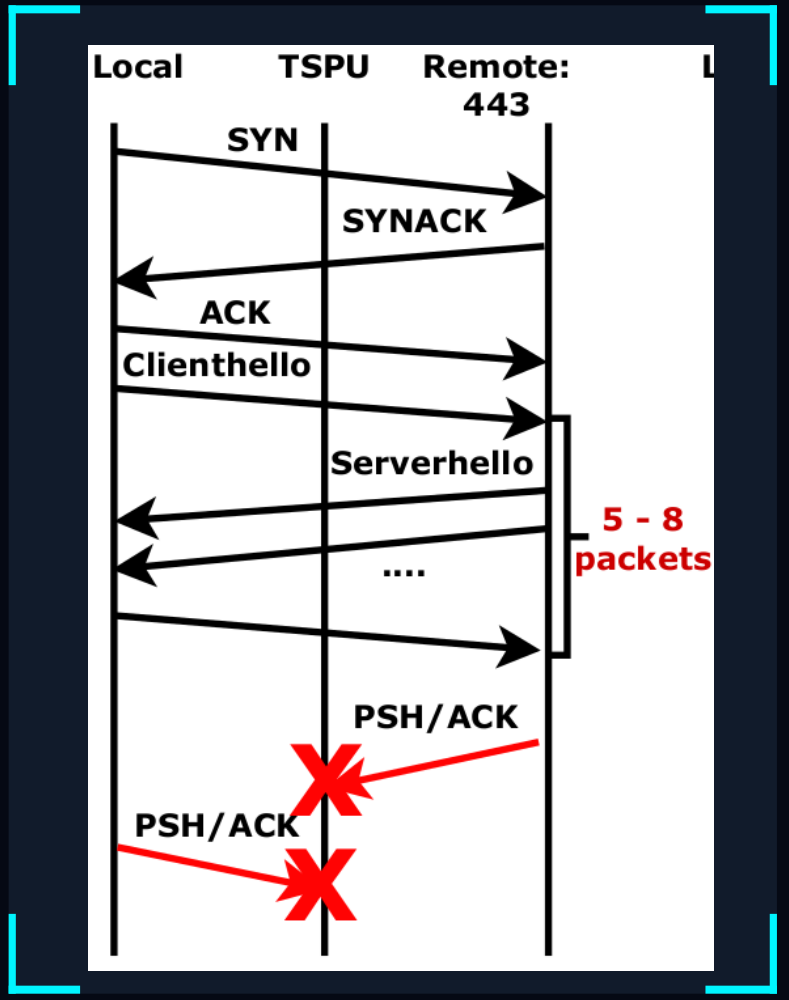


Bloqueos - SNI Based II

> Después del ClientHello deja pasar entre 5 y 8 paquetes más en cualquier dirección. A partir de ahí descarta todo en ambos sentidos

> La conexión se queda colgada (sin RST, simplemente deja de responder)

> Duración 420 segundos

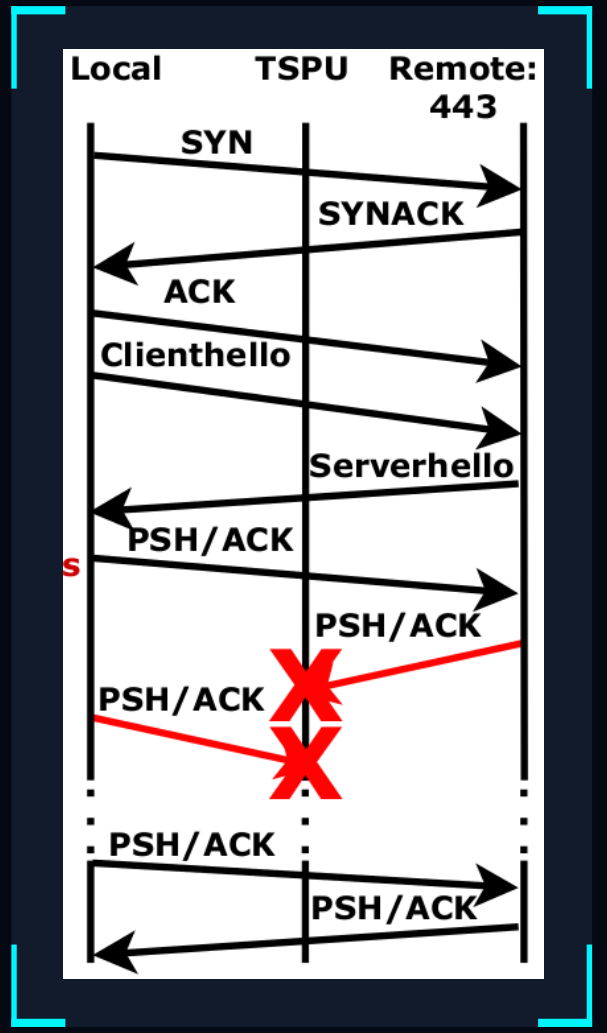


Bloqueos - SNI based III

> Del 26 de febrero al 4 de marzo de 2022

> Limitaba la velocidad a unos 600-700 bytes por segundo y descartaba lo que superaba ese límite. Es el mismo mecanismo que en el caso de Twitter de 2021

> El 4 de marzo en adelante se usa el SNI-I



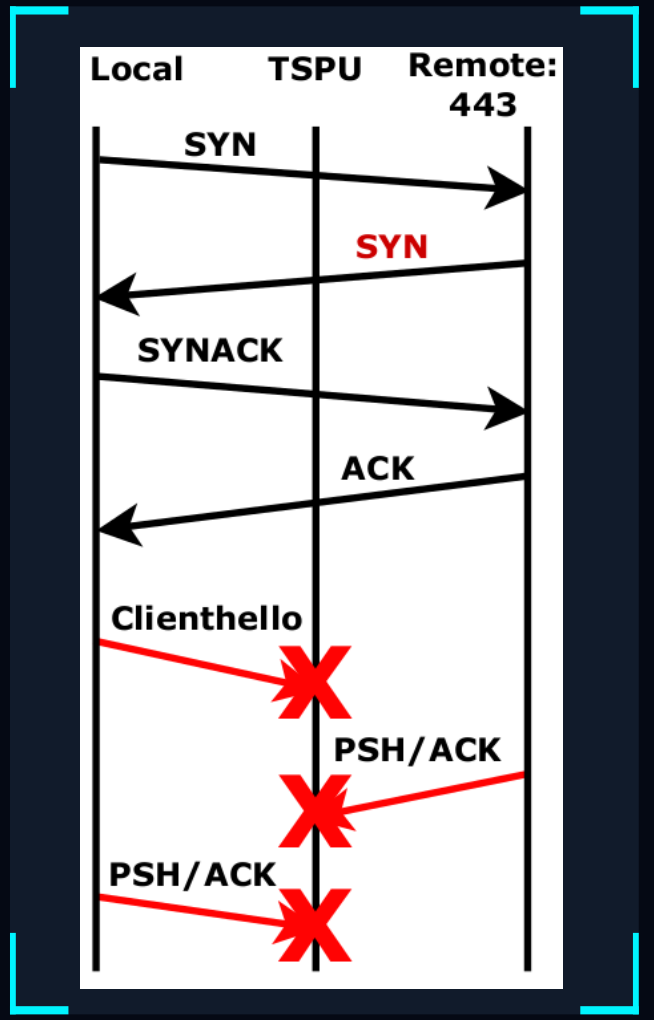
Bloqueos - SNI Based IV

> Descarta inmediatamente todos los paquetes de ambos lados, incluido el propio ClientHello

> Solo cuando **SNI-I no logra actuar**, por ejemplo con ciertas secuencias TCP raras como el **split handshake**, donde el servidor envía un SYN en vez de SYN/ACK

> Funciona como mecanismo de respaldo, parecido al de la Gran Muralla china

> Duración 40 segundos

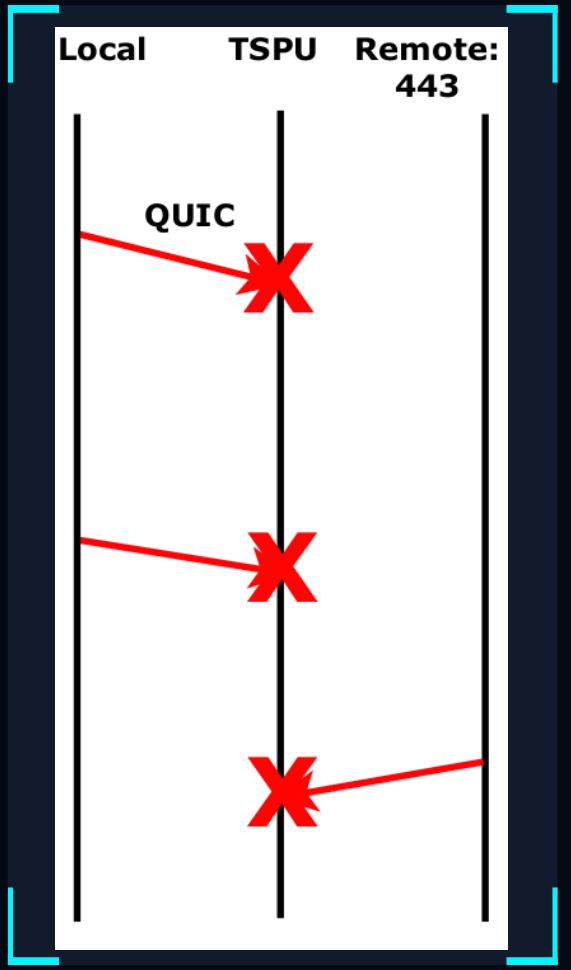


Bloqueos - QUIC

> Se inspecciona el primer paquete de cada flujo UDP

> El censor puede descifrarlo y leer el SNI
Si el dominio está prohibido, descarta el paquete (censura in-path), porque QUIC no permite inyectar resets como TCP)

> Durante 420 segundos. Cada paquete adicional reinicia el temporizador

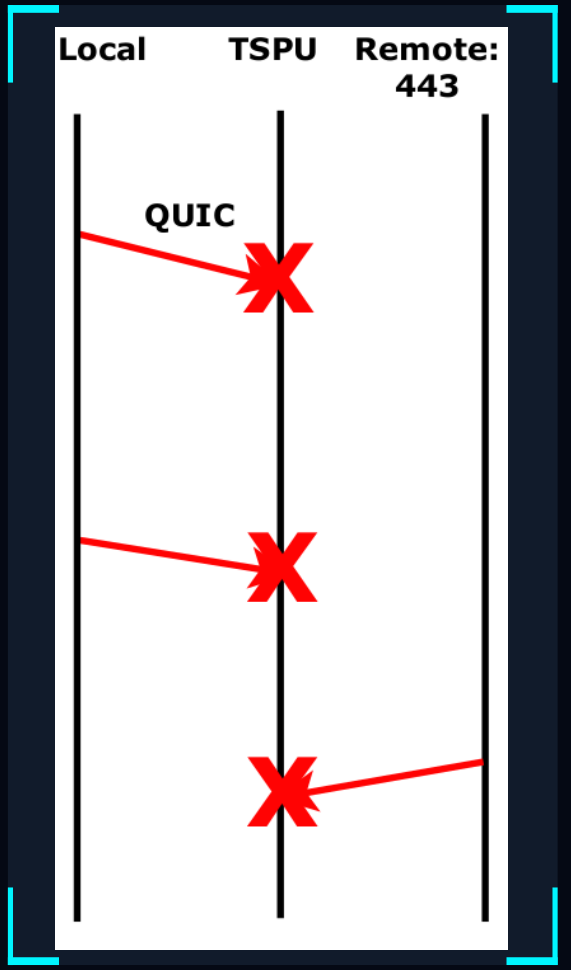


Bloqueos - QUIC

> Se aplicó censura al menos 9 meses antes que el Gran Cortafuegos chino (GFW), que se consideraba el primero

> Si el primer paquete no activa la censura, el resto de la conexión no se analiza

> Se ignora QUIC v2



Cronología Legal

2019 Ley de internet soberana (Runet)
2021 Ley de aterrizaje

> Obliga a las grandes empresas tecnológicas extranjeras a tener presencia legal en Rusia para poder operar allí. El nombre viene de que tienen que "aterrizar" en el país

Cronología Legal

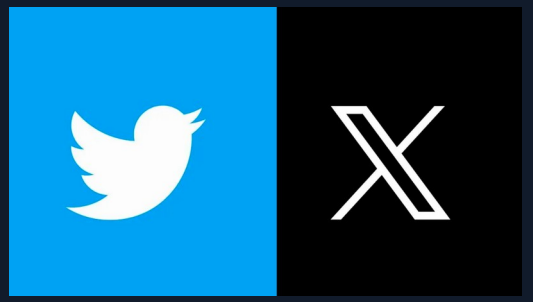
2019 Ley de internet soberana (Runet)
2021 Ley de aterrizaje
2021 Estrangulamiento de Twitter

> Se degradó su velocidad

> 100 % de las redes móviles y el 50 % de las fijas

> Twitter eliminó el 91 % del contenido solicitado

> Primer uso a escala nacional de estrangulamieno selectivo



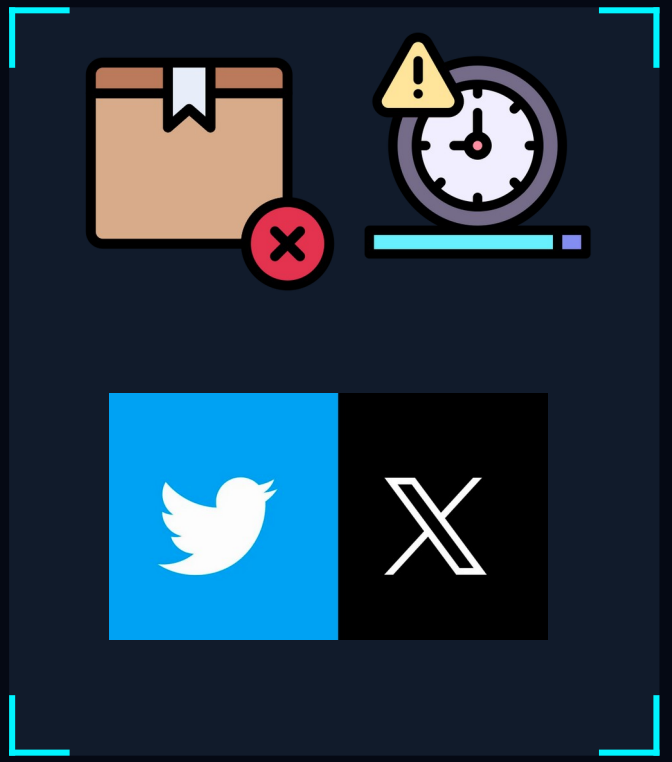
Estrangulamiento de Twitter

> Usa traffic policing en vez de traffic shaping
  130-150 kbps

> Primer paquete > 100 bytes, se deja de inspeccionar

> No reensambla registros TLS fragmentados

> Mantiene el estado de sesiones
  Inactivas unos 10 minutos
  Activas más de 2 horas



Cronología Legal

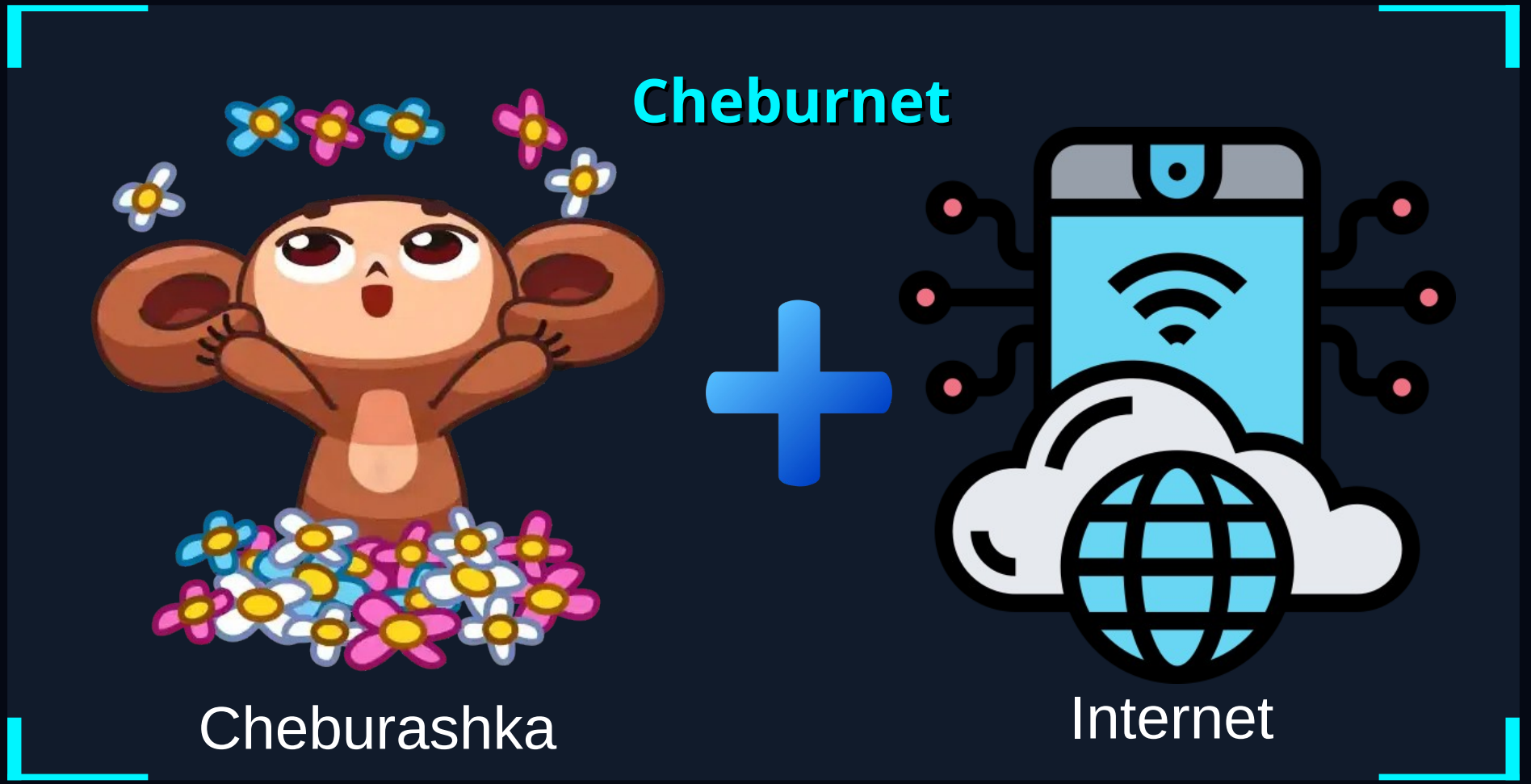
2019 Ley de internet soberana (Runet)
2021 Ley de aterrizaje
2021 Estrangulamiento de Twitter
2022 Leyes de guerra sobre noticias falsas

> Prohibición de palabras: guerra o invasión

> Bloqueos masivos

> El intento de secuestro BGP a Twitter

Evasión



Evasión - DNS

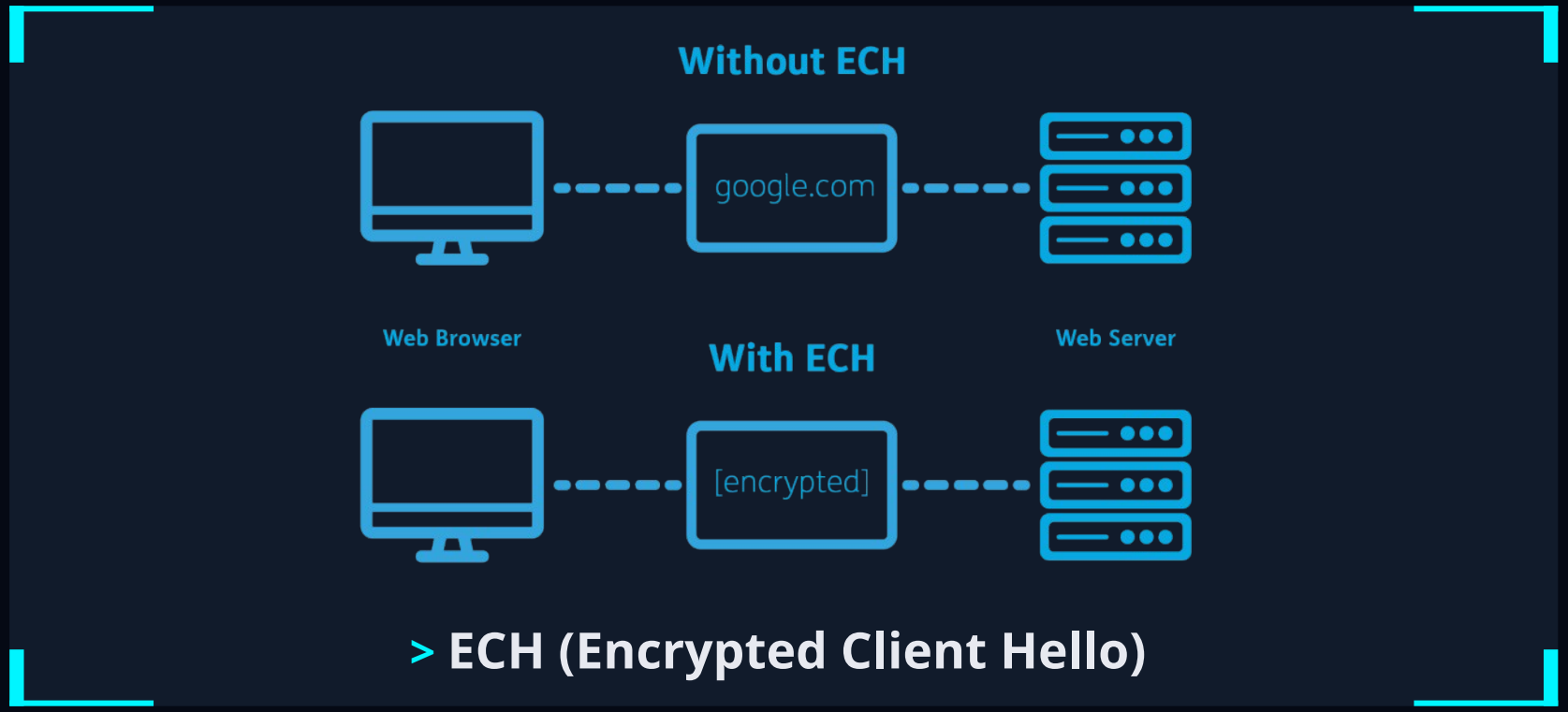


> DoH (DNS over HTTPS)

> DoT (DNS over TLS

>ODoH (Oblivious DNS over HTTPS)

Evasión - ECH



> ECH (Encrypted Client Hello)

Cronología Legal

2019 Ley de internet soberana (Runet)
2021 Ley de aterrizaje
2021 Estrangulamiento de Twitter
2022 Leyes de guerra sobre noticias falsas
2024 endurecimiento contra los VPNs, ECH, ...

> Bloquear determinadas VPNs

> Además, aplica análisis estadístico para identificar túneles VPN

> Bloqueo del ECH

Evasión

> Manipulación local de paquetes

> Ofuscación de protocolos VPN

> “Cooperativas de consumidores de Internet”





Cronología Legal

2019 Ley de internet soberana (Runet)
2021 Ley de aterrizaje
2021 Estrangulamiento de Twitter
2022 Leyes de guerra sobre noticias falsas
2024 endurecimiento contra los VPNs, ECH, ...
2025 Sobre la aprobación de las Reglas de gestión centralizada de la red de comunicaciones de uso público

> Decreto Sobre la aprobación de las Reglas de gestión centralizada de la red de comunicaciones de uso público. Kremlin le otorgó a Roskomnadzor la facultad legal para aislar la red rusa de la infraestructura global ante cualquier amenaza externa

> Bloqueo masivo de protocolos VPN, throttling a YouTube/WhatsApp/Telegram y pruebas de desconexión regional

Comparativa Rusia - UE



> Seguridad nacional, lucha contra el extremismo y soberanía digital

> TSPU centralizado en ISPs, bloqueos de medios/VPN sin orden judicial previa

> Prohibición de cifrado sin acceso **estatal; bloqueo de protocolos**

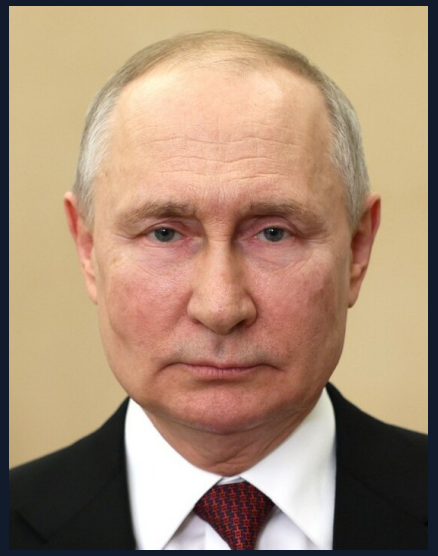


> Protección infantil (CSAM), lucha contra la desinformación y derechos de autor

> DSA (órdenes de retirada rápida), bloqueos DNS/IP por telecos, propuesta Chat Control

> Debate sobre Client-Side Scanning

Comparativa Rusia - España





Conclusiones:

> Rusia Exporta tecnologia de censura;
Uzbekistán, Tayikistán, Kazajistán, Kirguistán, Irán y Adganistán

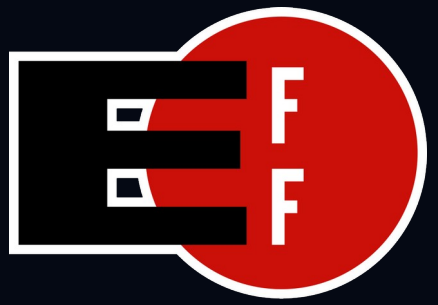
> Las herramientas técnicas “son neutras”

> Las capacidades de vigilancia y bloqueo siempre se expanden, nunca se desmontan

> Cifrado de extremo a extremo

Agradecimientos













Créditos visuales: Iconos diseñados por la comunidad de Flaticon (flaticon.es)

No se ha secado ningún río para hacer esta charla ;-)

¡Muchas gracias!

¿Preguntas?

