1- کاهش پهنای باند و مسدودسازی تدریجی نرم‌افزارها و پیام رسان‌های اجتماعی خارجی به ویژه اینستاگرام و واتس‌اپ - قطع یا اختلال مؤثر مکالمه صوتی و تصویری (LiveStream) اینستاگرام و واتس‌اپ

مبانی حقوقی و قانونی :

- مصوبه مورخ 96/9/10 مرکز ملی فضای مجازی (گام‌های اجرایی ساماندهی پیام‌رسان‌های اجتماعی) ☜ بندهای (2) و (1-2) ماده(1) بخش تکالیف حاکمیتی و ردیف(3) از وظایف وزارت ارتباطات در جدول «گام‌های اجرایی و برنامه‌زمان‌بندی مدیریت پیام‌رسان‌های خارجی» صورتجلسه شماره 9607 مورخ 96/10/9 مرکز ملی فضای مجازی
- بندهای (2) و (8) راهکارهای پیشنهادی گردشکار ستادکل نیروهای مسلح به مقام‌معظم رهبری
- بند (7) مصوبات مورخ 98/2/15 و بند (6) مصوبات مورخ 98/3/13 و بند (2) مصوبات مورخ 98/4/3 جلسات تشکیل شده در محضر ریاست قوه قضائیه
-بخشنامه شماره 9000/178439/100 – 1398/10/28 ریاست محترم قوه قضائیه موضوع ضرورت دریافت مجوز سرویسهای صوت و تصویر فراگیر از صدا و سیما
- دستورات متعدد قضایی صادره در این خصوص.

مبانی فنی و اجرایی :

طرح الف)- این اقدام از طریق تجهیزات اداره کل امنیت شبکه سازمان تنظیم مقررات به راحتی امکان پذیر است و این تدابیر فنی به صورت یکپارچه در ترافیک کلیه ارائه دهندگان خدمات دسترسی اعمال می‌گردد.

طرح ب) طبق بررسی‌های به عمل آمده در صورت عدم همکاری امنیت شبکه، با صدور دستور قضایی بطور مستقل از طریق اپراتورهای تلفن همراه که به تنهایی حدود 78 درصد سهم ترافیک اینترنت کشور را در اختیار دارند با استفاده از سازوکار **Traffic shaping** قابل اجرا می‌باشد. در اکثر اپراتورهای ثابت نیز چنین تجهیزاتی برای کنترل و مدیریت پهنای باند موجود است. با این وجود درخصوص شرکت‌های کوچک که ممکن است فاقد چنین تجهیزاتی باشند، مدیرعامل همراه اول در جلسه مشترک اعلام آمادگی نموده که تجهیزات مورد نیاز این شرکت‌ها را بطور امانی تأمین نماید.

ملاحظات:

اجرای طرح (ب) نیازمند اعلام قبلی به شرکت های ارائه دهنده خدمات ارتباطی ثابت (FCP) حداقل یک ماه قبل از شروع کار، برای تهیه و استقرار تجهیزات مورد نیاز است. این زمان برای آماده‌سازی و تنظیم تجهیزات مربوطه اپراتورهای تلفن همراه 2تا3 روز خواهد بود..

علاوه براین به منظور نظارت بر حسن اجرای این راهکار (طرح «الف» و «ب») نیازمند یک پیوست کنترلی از طریق دسترسی به سامانه امنیت شبکه برای نظارت و پایش مستمر (Live) ترافیک پهنای باند اپلیکیشن‌های موردنظر و میزان کاهش آن است. ضمناً باتوجه به اینکه تخطی هریک از ارائه دهندگان خدمات دسترسی در طرح(ب) مستقیماً موجب انتقال کاربران به خدمات دهنده خاطی و برهم زدن رقابت سالم شرکت‌ها خواهد شد.

لذا ضرورت دارد به‌صورت سازمان یافته با ایجاد نقاط دسترسی در هر یک از اپراتورهای ثابت و همراه در نقاط مختلف کشور، بر اعمال صحیح، یکپارچه و یکنواخت مدیریت پهنای باند پیام‌رسان‌های خارجی نظارت شود. در جلسات هماهنگی، سازمان اطلاعات سپاه پاسداران، برای انجام این مأموریت اعلام آمادگی نموده است.
ضمناً طبق بررسی انجام شده این اقدام حتما باید بطور همزمان با مسدودسازی فیلترشکن‌ها انجام شود والا موجب افزایش گرایش و مراجعه کاربران به ابزارهای گریز از فیلتر خواهد شد و هدف نهایی محقق نمی‌شود.

2- مسدودسازی کامل، مؤثر و مستمر کلیه فیلترشکن‌ها،VPN های غیرمجاز و ابزارهای گریز از فیلترینگ

مبانی حقوقی و قانونی :

-مصوبات مرکز ملی فضای مجازی (ابلاغیه شماره 01/91381/ش مورخ 91/11/1 و 22035/خ م مورخ 98/1/24)
-مصوبات متعدد کارگروه تعیین مصادیق محتوای مجرمانه
- مصوبات جلسات تشکیل شده در محضر ریاست قوه قضائیه (بندهای (3) و (9) جلسه مورخ 98/3/13 ، بندهای 3و5 جلسه مورخ 98/2/15)
-دستور قضایی دادسرای عمومی و انقلاب تهران مورخ 97/2/10

مبانی فنی و اجرایی:

- طبق بررسی‌های جامع به‌عمل آمده از جمله بررسی‌های انجام شده توسط هیأت سه نفره تحقیق دادستانی کل کشور (متشکل از نمایندگان سازمان بازرسی کل کشور و دادستانی کل و با سرپرستی آقای دکتر تقی‌پور وزیر اسبق ارتباطات و فناوری اطلاعات و عضو حقیقی شورای عالی فضای مجازی) که در سال 1397 انجام شد، مشخص گردید مسدودسازی اغلب غریب به اتفاق فیلترشکن‌ها از نظر فنی امکان‌پذیر است لیکن بنابه دلایل و توجیهاتی در حال حاضر انجام نمی‌شود. لذا ضرورت دارد با الزام قضایی، مسدودسازی کامل فیلترشکن‌ها از طریق مدیرکل امنیت شبکه و شرکت‌های پیمانکار فیلترینگ (شرکت یافتار پژوهان پیشتاز رایانش و شرکت داده پردازی دوران) بطور جدی پیگیری شود. براساس مصوبات جلسات ساماندهی فضای مجازی که در اوایل سال 98 در محضر ریاست قوه قضائیه برگزار گردید، مقرر گردید در صورت استنکاف و یا ناتوانی وزارت ارتباطات از مسدودسازی فیلترشکن‌ها ، با صدور دستور قضایی، این مسئولیت به سپاه پاسداران محول شود.
به‌عنوان راهکار جایگزین (درصورت عدم همکاری کامل امنیت شبکه) امکان استفاده از تجهیزات اپراتورهای تلفن همراه برای کاهش پهنای باند ناشناخته نیز وجود دارد. مسدودسازی یا کاهش پهنای‌باند این بخش از ترافیک شبکه، مستقیماً موجب افت کیفیت یا از کارافتادن نرم‌افزارهای فیلترشکن خواهد شد اما ممکن است موقتاً در برخی از سرویس‌های غیرفیلترشکن و مفید هم بطور ناخواسته اختلال ایجاد کند. لذا باتوجه به پیچیدگی عملکرد برخی از فیلترشکن‌ها نظیر سایفون، مسدودسازی کامل و دقیق ابزارهای گریز از فیلتر مستلزم همکاری امنیت شبکه و شرکت‌های پیمانکار فیلترینگ است.

3- واگذاری سامانه‌های فیلترینگ به ارائه‌دهندگان خدمات دسترسی و فراهم نمودن امکانات مربوط به نظارت قانونی و مستقیم دستگاه قضایی و دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه

مبانی حقوقی و قانونی :

– ماده 749 قانون مجازات اسلامی بخش تعزیرات که صراحتاً ارائه دهندگان خدمات دسترسی را به عنوان مجری فیلترینگ تعیین نموده است

- بند (3) راهکارهای پیشنهادی گردشکار ستادکل نیروهای مسلح به مقام معظم رهبری

مبانی فنی و اجرایی :

– علی رغم اینکه طبق قانون متولی فیلترینگ دستگاه قضایی (کارگروه تعیین مصادیق محتوای مجرمانه و مقامات قضایی) بوده و ارائه‌دهندگان خدمات دسترسی نیز به عنوان مجری فیلترینگ محسوب می‌شوند و سامانه‌های فیلترینگ با هزینه اپراتورهای تلفن همراه و برخی از ارائه‌دهندگان خدمات ارتباطی ثابت(FCP) تهیه و در مبادی ورودی آن‌ها نصب شده است اما در حال حاضر کنترل سامانه‌های فیلترینگ منصوبه ارائه‌دهندگان خدمات دسترسی، درانحصار واجا (امنیت شبکه) قرار دارد و این شرکت‌ها علی‌رغم مسئولیت قانونی، اختیارات و دسترسی لازم برای اعمال تکالیف قانونی خود در حوزه فیلترینگ را ندارند. لذا راهکار اجرایی برای احیاء ضوابط قانونی این است که اختیار هرگونه مداخله در حوزه فیلترینگ از سوی اداره کل امنیت شبکه سلب شده و به اپراتورها واگذار شود و دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه نیز در اجرای وظایف خود بطور مستقیم بر عملکرد سامانه‌های فیلترینگ و شرکت‌های پیمانکار آن نظارت نماید.

راهکار دوم که در صورت عدم همکاری امنیت شبکه و استنکاف از اجرای دستورات قضایی می‌توان اجرایی نمود، نصب و راه‌اندازی سامانه‌های جدید فیلترینگ در مبادی ارائه‌دهندگان خدمات دسترسی است. مشکل تأمین تجهیزات، تحمیل هزینه‌های مضاعف اجرای آن برای ارائه‌دهندگان خدمات دسترسی و تداخل عملکرد این سامانه‌ها و سامانه‌های امنیت شبکه از تبعات احتمالی این راهکار است.