



واکاوی آثار مخرب سوئیفت بر اقتصاد ایران و ارائه راهکارهای جایگزین



گزارش سیاستی شماره ۹۸۰۴۰۱

تیر ۱۳۹۸

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

وَالَّذِينَ جَاهَدُوا فِينَا لَنَهْدِيَنَّهُمْ سُبُلَنَا
وَأَنهَا كِه در راه ما (با خلوص نِيَّت) جهاد کنند،
قَطْعاً به راه‌های خود، هدايتشان خواهيم کرد

واکاوی آثار مخرب سوئفت بر اقتصاد ایران و ارائه راهکارهای جایگزین



واکاوی آثار مخرب سوئفت بر اقتصاد ایران و بررسی راهکارهای جایگزین

تولید و تجارت	گروه موضوعی:
سیاستی	نوع گزارش:
۱۳۹۸۰۴۳۰۶	شناسه:
۱۳۹۸/۰۴/۳۱	تاریخ انتشار:
حسین عطاءاللهی	تهیه و تدوین:
سید هادی رهگشای	مدیر مطالعه:
محمد امینی‌رعیا	ناظر علمی:

اندیشکده اقتصاد مقاومتی یک کانون تفکر با مأموریت «تصمیم سازی برای حل مسائل اقتصاد کشور در راستای تحقق اقتصاد مقاومتی» است که در سال ۱۳۹۵ فعالیت رسمی خود را آغاز نمود.

شناسایی شبکه مسائل در هر حوزه موضوعی، طراحی راهکار برای حل مسائل احصاء شده و هم‌اندیشی جهت ارزیابی و تدقیق آن، بررسی تجربیات جهانی، طرح مباحث در فضای نخبگانی و رسانه‌ای و پیگیری راهکارهای ارائه شده از دستگاه‌ها و مسئولین مرتبط به منظور اتخاذ تصمیمات لازم، از جمله فعالیت‌هایی است که در اندیشکده انجام می‌شود.

علاقه‌مندان می‌توانند از طریق سایت Mett.ir با اندیشکده اقتصاد مقاومتی در ارتباط باشند و نظرات، انتقادات و پیشنهادهای خود را در خصوص این گزارش و همچنین سایر فعالیت‌های اندیشکده، ارائه نمایند.

فهرست

۸..... خلاصه مدیریتی

بخش اول

۱۲..... مقدمه

بخش دوم

۱۴..... معرفی سوئیفت و کارکردهای آن

بخش سوم

۱۶..... رصد اطلاعات مالی کشورها از طریق سوئیفت توسط آمریکا

بخش چهارم

۲۱..... شکایت کشورها از سوئیفت به دلیل جاسوسی آمریکا

بخش پنجم

۲۷..... جاسوسی مشترک پس از تفکیک سوئیفت میان اروپا و آمریکا

بخش ششم

۳۱..... کارکردهای سوئیفت برای آمریکا

بخش هفتم

۳۳..... آسیب‌های سوئیفت برای اقتصاد ایران

بخش هشتم

۳۶..... گسترش پیام‌رسان‌های موازی سوئیفت در جهان و واکنش آمریکا

بخش نهم

۴۴..... پیشنهادها

خلاصه مدیریتی

وزارت خزانة داری آمریکا به عنوان اتاق جنگ اقتصادی این کشور، اقدامات متعددی جهت ایجاد فشار اقتصادی و تغییر مسیر جمهوری اسلامی ایران، انجام داده است. بررسی و واکاوی این اقدامات نشان می‌دهد که این وزارتخانه، تا چه حد برای اثرگذاری تحریم‌ها علیه ایران تلاش می‌نماید و بر آن متمرکز است. یکی از راهکارهای مهم و اساسی اتاق جنگ آمریکا برای فشار اقتصادی به ایران، ایجاد محدودیت برای مبادلات مالی بین‌المللی کشور بوده است تا از این طریق، روابط تجاری ایران را محدود و پرهزینه نماید. در این راستا، این نهاد از پیام‌رسان سوئیفت برای اعمال محدودیت و تحریم علیه ایران استفاده کرده است؛ سامانه‌ای که نزد مسئولین آمریکایی، از آن به عنوان یکی از عناصر مهم اثرگذاری تحریم‌ها یاد می‌شود.

سوئیفت به عنوان یک پیام‌رسان مالی، کارکردی مشابه پست الکترونیکی یا پیام کوتاه دارد. در واقع سوئیفت به تنهایی عملیات بانکی و مالی اعم از انتقال وجه، افتتاح حساب، تسویه و غیره انجام نمی‌دهد؛ بلکه صرفاً وظیفه انتقال داده‌ها و پیام‌های مربوط به عملیات مالی بانکی را بر عهده دارد. به صورت ساده شده می‌توان گفت زمانی که یک انتقال مالی قرار است بین دو بانک خارجی انجام شود، دستور پرداخت حاوی یک پیام از بانک اول به سوئیفت ارسال شده و در صورت تایید، این دستور به بانک دوم ارائه می‌گردد؛ سپس بانک دوم نیز در پیامی که همین مسیر را به صورت برعکس طی می‌کند، پاسخ بانک اول را داده و مبادله انجام می‌شود. در نتیجه تمامی مبادلات جهانی که در حال حاضر در قالب پیام‌رسان سوئیفت انجام می‌گیرد، در پایگاه داده‌های این پیام‌رسان ثبت شده و قابل ردیابی است.

پس از جریان ۱۱ سپتامبر، دولت آمریکا از طریق وزارت خزانة داری این کشور و در قالب برنامه «ردیابی تأمین مالی تروریسم»، عملاً مجوز دسترسی به اطلاعات مالی مردم

و کشورهای جهان در سوئیفت و جاسوسی از آن را از این نهاد دریافت نمود؛ اقدامی که تا مدت‌ها حتی از نظر کشورهای اروپایی پنهان ماند. از آن زمان تاکنون، با وجود اعتراضات متعدد کشورهای جهان و نقض قوانین و حریم خصوصی افراد، آمریکا کماکان به داده‌های سوئیفت دسترسی داشته و شریان‌های اقتصادی کشورها را از طریق این پیام‌رسان شناسایی و در مواقع لازم، آنها را مورد تحریم قرار می‌دهد.

پیش از سال ۱۳۹۰ و دوره اول تحریم‌ها، سوئیفت به آمریکا کمک کرد تا این کشور بتواند تمام جریان مالی ایران را شناسایی کند؛ سپس ایران را از مسیرهای شناسایی شده تحریم نماید و با قطع دسترسی به سوئیفت، زمینه را برای قفل کردن مبادلات مالی کشور فراهم کند. هر چند تحریم سوئیفت، مراودات بین‌المللی بانک‌های ایرانی را متوقف نکرد، اما هزینه‌های زیادی بر عملیات ارزی و بانکی کشور تحمیل نمود. این اقدام نشان داد که کشورهای اروپایی و آمریکا که سکناداران اصلی سوئیفت هستند، نه تنها از داده‌های سوئیفت به نفع خود و علیه کشورها استفاده می‌کنند، بلکه با سوءاستفاده از این ابزار، کشورها را از طریق آن تحت تحریم‌های بانکی قرار می‌دهند.

اما با دستیابی به توافق هسته‌ای موسوم به برجام بین ایران و کشورهای گروه ۱+۵ در تاریخ ۲۷ دی ۱۳۹۴ و اجرای آن، تحریم سوئیفت از ایران برداشته شد. پس از لغو این تحریم، بانک‌های تجارت، رفاه کارگران، توسعه صادرات، سپه، پست بانک، صنعت و معدن، بانک ایران و اروپا، بانک توسعه تعاون، سینا، ملت و ملی به سوئیفت متصل شدند؛ بانک مرکزی نیز به دنبال افزایش به کارگیری سوئیفت توسط بانک‌های ایرانی بود و آمار پیام‌های رد و بدل شده در این پیام‌رسان را به عنوان یک «دستاورد مهم» ارائه می‌نمود. با بازگشت دوباره ایران به سوئیفت، مجدداً این امکان در اختیار آمریکا قرار گرفت که مبادلات مالی و مسیرهای جدید کشور را رصد نماید. این اقدام نیز در

نهایت به تحریم‌های سال ۱۳۹۷ و تهدید ایران به اخراج از سوئیفت و قطع دسترسی کشور به این پیام‌رسان منجر شد و ضربه ای دیگر از سوئیفت به کشور وارد گردید.

در واقع آمریکا از ابزار سوئیفت به دو شکل علیه ایران استفاده نموده است. شکل اول، رصد مبادلات ایران است؛ دولت آمریکا با دسترسی غیرقانونی که به سوئیفت و داده‌های آن دارد، این امکان را دارد تا همه مبادلات انجام شده در آن را رصد نماید و از وضعیت کشورهای مدنظر خود از جمله ایران، در مبادلات جهانی شان اطلاع یابد. شکل دوم نیز تهدید ایران به قطع سوئیفت است که منجر به ایجاد اختلال در مبادلات بانکی کشور می‌شود؛ در واقع از آنجا که پیام‌رسانی مبادلات مالی ایران از طریق سوئیفت انجام می‌شود، قطع این دسترسی، ایران را در انجام تجارت با کشورها و فرآیندهای مالی آن با مشکل مواجه می‌کند. با این وجود، اقدام راهبردی و قابل توجهی طی این سال‌ها توسط بانک مرکزی، جهت کاهش وابستگی به سوئیفت انجام نشده و این نهاد برخلاف منطق اقتصادی و امنیتی، همواره به دنبال ایجاد تسهیل در استفاده مجدد از این پیام‌رسان بوده است.

عدم اقدام بانک مرکزی در این زمینه، در شرایطی رقم خورده است که طی سال‌های اخیر، کشورهای مختلف اقدامات گسترده‌ای به منظور کاهش استفاده از سوئیفت و خروج از این پیام‌رسان انجام داده‌اند. در این زمینه کشورهایی از قبیل چین و روسیه پیشرو بوده و سامانه‌های پرداخت بومی و مخصوص خود را ایجاد کرده اند تا از آن در تبادلات با کشورها استفاده نمایند. همچنین سایر کشورها و بانک‌های بزرگ بین‌المللی نیز به تناسب نیاز خود، استفاده از پیام‌رسان مالی موازی سوئیفت را در دستور کار قرار داده‌اند. البته آمریکا نیز در واکنش به اقدامات متعدد کشورها در کاهش وابستگی به سوئیفت و به حداقل رساندن استفاده از این پیام‌رسان، منفعل عمل نکرده است؛ و با تقویت کارگروه ویژه اقدام مالی یا همان FATF، به دنبال شیوه‌های جدید در کسب اطلاعات مالی و تجاری کشورهای جهان است.

با این اوصاف، ضروری است جمهوری اسلامی ایران نیز که بیشترین تاثیر منفی را از تحریم‌های یکجانبه و ظالمانه آمریکا و وابستگی به سوئیفت دریافت کرده، هرچه سریعتر به سمت استفاده از راهکارهای جایگزین و موازی حرکت نماید؛ در این میان، بانک مرکزی اصلی‌ترین نهادی است که باید در این جنگ اقتصادی نقش آفرینی داشته باشد. راه اندازی و استفاده از پیام‌رسان مالی اختصاصی در همکاری دوجانبه و چندجانبه با سایر کشورها یا اتحادیه‌ها، استفاده از ظرفیت پیام‌رسان ملی سپام در تبادلات داخلی و بین‌المللی و ایجاد دسترسی برای بانک‌ها و مؤسسات مالی خارجی طرف قرار داد با بانک‌های ایرانی، انعقاد قرارداد همکاری با کشورها، مجامع، اتحادیه‌ها، بانک‌ها و مؤسسات مالی منطقه‌ای و بین‌المللی که در زمینه ایجاد پیام‌رسان‌های مالی موازی سوئیفت اقدام کرده اند و تأمل و احتیاط بیشتر در پیوستن به FATF در چارچوب فعلی همکاری این نهاد، از جمله اقداماتی است که باید در این راستا در دستور کار قرار گیرد.

بخش اول

مقدمه

وزارت خزانه داری آمریکا به عنوان اتاق جنگ اقتصادی این کشور، اقدامات متعددی جهت ایجاد فشار اقتصادی و تغییر مسیر جمهوری اسلامی ایران، انجام داده است. بررسی و واکاوی این اقدامات نشان می‌دهد که این وزارتخانه، تا چه حد برای اثرگذاری تحریم‌ها علیه ایران تلاش می‌نماید و بر آن متمرکز است.

یکی از راهکارهای مهم و اساسی اتاق جنگ آمریکا برای فشار اقتصادی به ایران، ایجاد محدودیت برای مبادلات مالی بین‌المللی کشور بوده است تا از این طریق، روابط تجاری ایران را محدود و پرهزینه نماید. در این راستا، این نهاد از پیام‌رسان سوئیفت برای اعمال محدودیت و تحریم علیه ایران استفاده کرده است؛ پیام‌رسانی که نزد مسئولین آمریکایی، از آن به عنوان یکی از عناصر مهم اثرگذاری تحریم‌ها یاد می‌شود.

به عنوان نمونه اخیراً جیمز ریکاردز مشاور سازمان CIA آمریکا و از طراحان اصلی تحریم‌ها علیه ایران، بیان کرده است که آمریکا از طریق دلار و نظامات پرداختی آن به تمامی مبادلات کشورها اشراف کامل دارد و تحریم‌های آمریکا بدون دلار و نظاماتی مانند سوئیفت مؤثر نخواهد بود.

آمریکا از ابزار سوئیفت استفاده دو وجهی می‌نماید. وجه اول، رصد مبادلات ایران است؛ دولت آمریکا با دسترسی غیرقانونی که به سوئیفت و داده‌های آن پیدا کرده، این امکان را دارد تا همه مبادلات انجام شده در آن را رصد نماید و از تبادلات مالی کشورهای مدنظر خود از جمله ایران، اطلاع یابد. این نوع بهره‌برداری از سوئیفت، زمینه را برای تحریم و اثرگذاری آن فراهم می‌کند. وجه دوم، تهدید ایران به قطع سوئیفت است که منجر به ایجاد اختلال در مبادلات بانکی کشور می‌شود؛ در واقع از آنجا که پیام‌رسانی مبادلات مالی ایران تاکنون از طریق سوئیفت بوده است، قطع

این دسترسی، ایران را در تجارت با کشورها و فرآیندهای مالی آن با مشکل مواجه می‌نماید.

بنابراین چه حضور ایران در سوئیفت و چه ممنوع شدن استفاده از آن، برای کشور هزینه‌زا بوده و دولت آمریکا در هر دو صورت، با این ابزار مالی ایران را تحت فشار قرار داده است. با این حال، پس از سوء استفاده آمریکا از سوئیفت علیه ایران در جریان تحریم‌های سال ۹۰-۹۱ به شکلی که توضیح داده شد، بانک مرکزی تلاش قابل توجهی برای کاهش وابستگی به این ابزار اطلاعاتی انجام نداد و سوئیفت، مجدداً در تحریم‌های سال ۱۳۹۷ برای ایران مشکل‌ساز شد. در واقع بانک مرکزی پس از برجام، مجدداً به دنبال بازگشت به سوئیفت بود و افزایش مبادلات انجام شده از طریق این پیام‌رسان را به عنوان موفقیت گزارش می‌داد؛ حال آنکه نگاه به ماهیت این ابزار و اقدامات دیگر کشورها در کاهش وابستگی به آن، به خوبی نمایان می‌نمود که چنین مسیری اشتباه است.

در این شرایط، ضروری است جمهوری اسلامی ایران هرچه سریعتر تدابیر لازم را در کاهش وابستگی به سوئیفت و استفاده از ابزارهای موازی اتخاذ نماید. هرچند طبق گفته‌های اخیر مسئولین بانک مرکزی، پیام‌رسان‌های موازی سوئیفت در حال به کارگیری است، اما این مسیر باید به صورت دائمی و نه مقطعی، در دستور کار قرار گیرد.

در گزارش حاضر، ضمن بررسی شیوه پیام‌رسانی مالی بین‌المللی که از طریق سوئیفت انجام می‌شود، نحوه نظارت آمریکا بر این پیام‌رسان و رصد تراکنش‌های مالی کشورها از طریق آن مورد واکاوی قرار گرفته و استفاده دو وجهی این کشور از سوئیفت برای فشار به کشورهای غیرهمسو، تشریح شده است؛ مسئله‌ای که جمهوری اسلامی ایران بیشترین تاثیر نامطلوب را از آن پذیرفته است. در ادامه نیز به سیر تحولات بین‌المللی و راهکارهای کشورها و بانک‌ها در حوزه پیام‌رسانی مالی و شکل‌گیری پیام‌رسان‌های موازی سوئیفت پرداخته شده و در نهایت، رویکرد ایران و راهکارهای موجود برای مقابله با تهدیدات سوئیفت در قالب پیشنهادها و سیاستی ارائه گردیده است.

بخش دوم

معرفی سوئیفت و کارکردهای آن

بعد از خاتمه جنگ جهانی دوم و در اواخر دهه ۱۹۵۰، رشد تجارت جهانی باعث افزایش حجم تبادلات بین‌المللی شد؛ اما از آنجا که در ابتدا بانک‌ها و مؤسسات مالی از روش تلکسی برای تبادل اطلاعات مالی استفاده می‌کردند، به دلیل نبود استانداردهای بین‌المللی در محاورات بین بانکی، پرداخت‌های بین‌المللی دچار آشفتگی و هزینه بالا بود. از این رو در اوایل دهه ۱۹۶۰ حدود ۶۰ بانک بزرگ اروپایی و آمریکایی به این فکر افتادند که پیام‌های بین بانکی را به نحوی طرح‌ریزی و استاندارد کنند که اتوماسیون نظام بانکی بین‌المللی را به همراه داشته باشد.

در دسامبر سال ۱۹۶۷ هفت بانک معتبر از کشورهای آمریکا، اتریش، انگلستان، دانمارک، سوئیس، فرانسه و هلند مطالعه‌ای را شروع کردند و در سال ۱۹۷۱، ۷۳ بانک از این کشورها هزینه مطالعه را تقبل کردند. این مطالعه به همت گروهی از متخصصان و به مدت یک سال طول کشید و نتایج آن در سال ۱۹۷۲ ارائه شد. به دنبال مطالعات صورت گرفته، در نهایت در ماه می ۱۹۷۳، سوئیفت^۱ یا انجمن ارتباطات مالی بین بانکی با عضویت ۲۳۹ بانک از ۱۵ کشور در شهر لاهولپ در نزدیکی بروکسل پایتخت کشور بلژیک با دو هدف استانداردگذاری و پردازش مبادلات بانکی بین‌المللی تأسیس شد. سوئیفت به عنوان یک شرکت، دارای ساختاری است که در آن هر یک از سهامداران، مالک و ناظر شرکت محسوب می‌شوند^۲.

سوئیفت با این هدف شکل گرفت که محیطی مطمئن، سریع، استاندارد و قابل اعتماد را برای ارتباط فعالان در دنیای مالی ارائه کند. عملیات سوئیفت طبق گفته مسئولین آن، عرضه امن خدمات برای انتقال پیام و نرم‌افزارهای واسط ارتباطی است. با توجه به

1. Society for Worldwide Interbank Financial Telecommunication (SWIFT)

2. Swift.com/about_swift

ماده ۳ اساسنامه سوئیفت، هدف اصلی این شرکت در راستای منافع کل اعضای شرکت بوده و بهره‌برداری از امکانات لازم برای ارتباط از راه دور، انتقال و مسیریابی پیام‌های خصوصی، محرمانه و اختصاصی مالی را شامل می‌شود.

در مجموع سوئیفت به عنوان پیام‌رسان مالی، کارکردی مشابه پست الکترونیکی یا پیام کوتاه دارد. در واقع سوئیفت به تنهایی عملیات بانکی و مالی اعم از انتقال وجه، افتتاح حساب، تسویه و غیره انجام نمی‌دهد؛ بلکه صرفاً وظیفه انتقال داده‌ها و پیام‌های مربوط به عملیات مالی بانکی را بر عهده دارد. به صورت ساده شده می‌توان گفت زمانی که یک انتقال مالی قرار است بین ۲ بانک خارجی انجام شود، دستور پرداخت حاوی یک پیام از بانک اول به سوئیفت ارسال شده و در صورت تایید، این دستور به بانک دوم ارائه می‌گردد؛ سپس بانک دوم نیز در پیامی که همین مسیر را به صورت برعکس طی می‌کند، پاسخ بانک اول را داده و مبادله انجام می‌شود. در نتیجه تمامی مبادلات جهانی که در حال حاضر در قالب پیام‌رسان سوئیفت انجام می‌گیرد، در پایگاه داده‌های این پیام‌رسان ثبت شده و قابل ردیابی است. در واقع محور اصلی و اساس کار سوئیفت، ذخیره و ارسال پیام‌های مرتبط با تبادلات مالی است. سوئیفت در بیش از ۲۰۰ کشور، بیش از ۱۱ هزار مؤسسه مالی را قادر می‌سازد تا مبادله داده‌های مالی را انجام دهند. این پیام‌ها به صورت ارسال کاربر به کاربر، کاربر به سوئیفت و سوئیفت به کاربر امکان‌پذیر است. علاوه بر مکان اصلی سوئیفت که در بلژیک مستقر است، سوئیفت در کشور هلند و آمریکا نیز مرکز داده ایجاد کرده است که به صورت کاملاً متقارن عمل می‌کنند. بدین صورت که هر پیام مالی که درون سوئیفت انتقال می‌یابد، در هر دو این مراکز داده ذخیره می‌شود. انگلیس و هنگ کنگ نیز به عنوان مراکز پشتیبان اعضا، بعدها فعالیت خود را آغاز کرده‌اند. تعاونی سوئیفت نرم‌افزار رابط میان مؤسسات مالی جهان را ارائه می‌دهد. هر چند این تعاونی خود یک بانک نیست و هیچ حسابی از سپرده‌گذاران نگهداری نمی‌کند، اما به عنوان «مرکز عصبی» بانک‌های جهان عمل می‌نماید.

بخش سوم

رصد اطلاعات مالی کشورها از طریق سوئفت توسط آمریکا

بعد از حادثه ۱۱ سپتامبر، جورج بوش رئیس جمهور آمریکا در واکنش به حملات تروریستی، در این کشور وضعیت اضطراری ملی اعلام کرد. همزمان با این اقدامات، بوش برای پیشگیری از حملات احتمالی آتی، فرمان اجرایی ۱۳۲۲۴ را نیز صادر نمود که بر اساس آن، به وزارت خزانه داری آمریکا قدرت و اختیاراتی اعطا شده بود. هدف از این اقدام، استفاده از تمام روش‌ها برای شناسایی، پیشگیری و پیگیری کسانی بود که اقدامات تروریستی در داخل و خارج از این کشور انجام می‌دادند. اما علاوه بر این، افرادی که حمایت مالی و یا سایر فعالیت‌های تروریستی را ارائه می‌دادند نیز مورد هدف این قانون قرار گرفتند.

وزارت خزانه‌داری آمریکا در شروع استفاده از اختیارات خود برای شناسایی، نظارت و پیگیری تروریست‌های مظنون و همچنین افراد و سازمان‌هایی که مشکوک به تأمین مالی تروریست‌ها بودند، «برنامه ردیابی تأمین مالی تروریسم»^۱ را در دستور کار قرار داد. رئیس جمهور آمریکا برای صدور دستورالعمل اجرایی و سپس اعطای این اختیار به وزارت خزانه‌داری طبق برنامه مذکور، به «قانون اختیارات اقتصادی بین‌المللی»^۲ و «قانون مشارکت سازمان ملل متحد»^۳ استناد نمود.

بر اساس قانون اختیارات اقتصادی بین‌المللی، رئیس جمهور آمریکا در وضعیت اضطراری و وجود یک تهدید فوق‌العاده برای آمریکا، از دایره اختیارات گسترده‌تری برخوردار است. از جمله این اختیارات می‌توان به توانایی دسترسی به معاملات مالی یا نقل و انتقالات بین مؤسسات بانکی (که شامل هر گونه تبادلات افراد یا کشورهای

1. Terrorist Finance Tracking Program (TFTP)
2. International Emergency Economic Powers Act (IEEPA)
3. United Nations Parliamentary Assembly (UNPA)

خارجی می‌شود) اشاره کرد. همچنین بر اساس قانون مشارکت سازمان ملل متحد، رئیس جمهور آمریکا مجاز است مطابق با مقررات شورای امنیت سازمان ملل متحد، اقداماتی را انجام دهد؛ این مقررات شامل نظارت بر روابط مالی و معاملات بین افراد و کشورهای خارجی با آمریکا می‌شود.

آغاز دسترسی آمریکا به سوئیفت برای ردیابی تأمین مالی تروریسم

زمانی که برنامه ردیابی تأمین مالی تروریسم در دستور کار دولت آمریکا قرار گرفت، اعضای دولت بوش از میزان اطلاعات مالی موجود در پایگاه داده‌های سوئیفت اطلاعی نداشتند و از این رو، تا مدت‌ها دریافت اطلاعات از نظام پرداخت سوئیفت، در برنامه ردیابی تأمین مالی تروریسم آمریکا مطرح نشد؛ تا اینکه یک مدیر اجرایی از وال استریت با یکی از اعضای کلیدی دولت این موضوع را مطرح کرد که «دسترسی به پایگاه داده‌های سوئیفت، می‌تواند یک منبع ارزشمند برای ردیابی مسیرهای تأمین مالی و مبادلات جهانی باشد». این پیشنهاد با استقبال فراوان دولت آمریکا مواجه شد، به خصوص به این دلیل که شواهد نشان می‌داد در حادثه ۱۱ سپتامبر ۹ نفر از ۱۱ نفر، برای کمک و تأمین مالی طرحشان از طریق نظام نقل و انتقالات بین‌المللی، به صورت رسمی پول دریافت کرده‌اند. در آن زمان این پول‌ها از بانک‌های اروپایی و آسیایی به آمریکا فرستاده شده بود.^۱

به محض اینکه دولت آمریکا متوجه شد که می‌تواند فعالیت‌های بانکی در سطح جهان را با دسترسی به سوابق حساب‌های مالی سوئیفت که شامل اطلاعات مربوط به نقل و انتقالات بین‌المللی بود، شناسایی و نظارت کند، از طریق وزارت خزانه‌داری و به وسیله «احضاریه‌های اداری»^۲ شروع به بهره‌برداری از داده‌های سوئیفت نمود. استفاده از احضاریه‌های اداری که پاسخ به آن اجباری بود، یک مفهوم جدید طراحی شده

1. Scholarship.law.unc.edu/ncbi/vol11/iss1/16/

2. Administrative Subpoena

توسط خزانه داری آمریکا برای دور زدن رویه‌های معمول قضائی بود؛ در حالی که طبق رویه‌های معمول، دسترسی به سوابق مالی اشخاص معمولاً از طریق صدور احضاریه‌ای که برای اولین بار توسط یک هیأت منصفه بزرگ و توسط دستگاه‌های قضائی تأیید شده بود، صورت می‌پذیرفت.

در اصل مقامات وزارت خزانه‌داری به موجب مجوزهای صادره از طرف رئیس جمهور تحت قانون اختیارات اقتصادی بین‌المللی، احضاریه خود را به مقامات سوئیفت جهت دسترسی به سوابق مالی افراد ارائه می‌دادند. هدف از این اقدامات، جستجو در پایگاه داده‌های سوئیفت به منظور کشف روابط مالی مدنظر آمریکا عنوان می‌شد.

توافق مخفی آمریکا با سوئیفت برای دسترسی به تمام اطلاعات

سوئیفت روزانه میلیون‌ها پیام از طریق شبکه جهانی خود منتقل می‌کند؛ پیام‌هایی که شامل دستورالعمل‌های دقیقی در مورد نحوه انتقال پول و دیگر اوراق بهادار است. از آنجایی که سوئیفت، کسب و کار و عملیات قابل توجهی در آمریکا دارد و تحت مجوز بانک مرکزی آمریکا به فعالیت می‌پردازد، از این رو این نهاد مجبور به همکاری با آمریکا در پاسخ به «احضاریه‌های اداری» گردید.

آمریکا از طریق «دفتر کنترل دارایی‌های خارجی»^۱ که زیرمجموعه وزارت خزانه داری این کشور قرار دارد، به عنوان بخشی از توافق مخفی خود با سوئیفت در زمان دولت بوش، یک دستورالعمل اجباری را به سوئیفت جهت دسترسی به سوابق مالی مشتریان فرستاد. در این دستورالعمل از سوئیفت خواسته شده بود به منظور دسترسی آمریکا به اطلاعات تروریست‌ها، برخی اطلاعات مالی مشتریان، شامل اطلاعاتی که نشانگر هویت فرستنده و گیرنده پیام مالی بود را در اختیار آمریکا قرار دهد. این اطلاعات همچنین شامل شماره حساب بانکی هر یک از طرفین و مقدار وجه مورد معامله و

1. Office of Foreign Assets Control (OFAC)

اقلام متعدد اطلاعاتی دیگری نیز بود^۱.

اما آمریکا از ارتباط با سوئیفت و دسترسی به اطلاعات مالی کشورهای جهان از طریق آن، تنها به منظور شناسایی تأمین مالی تروریسم استفاده نکرد. بلکه این برنامه روشی جهت دستیابی به اطلاعات مهم مالی افراد مختلف بود که در آن نیازی به حکم یا اجازه قاضی، یا رعایت قانون حفظ حریم خصوصی در دسترسی به اطلاعات شخصی افراد نبود.

میزان دستیابی آمریکا به اطلاعات سوئیفت

مقامات آمریکا در استفاده از داده‌های سوئیفت، بلافاصله اطلاعات جمع‌آوری شده مربوط به یک مظنون خاص را مورد هدف قرار نمی‌دادند. آنها ابتدا اطلاعات انبوهی از پیام‌های سوئیفت در ارتباط با یک مظنون در منطقه جغرافیایی خاص و زمان مشخص را درخواست می‌کردند؛ سپس طیف گسترده‌ای از این پیام‌ها را از سوئیفت دریافت و به پایگاه جستجوگر داده‌های وزارت خزانه‌داری آمریکا ارسال می‌نمودند. در نهایت تحلیلگران برنامه ردیابی تأمین مالی تروریسم آمریکا، از ابزارهای خود برای جستجوهای خاص در مقیاس بزرگ استفاده نموده تا پیام‌های مربوط به سوئیفت را باز کنند.

نمایندگان وزارت خزانه‌داری آمریکا به طور مداوم ادعا می‌کردند که داده‌های ارائه شده توسط سوئیفت، تنها برای استخراج اطلاعاتی که به تحقیقات تروریستی منتهی می‌شود، مورد استفاده قرار می‌گیرند. از طرفی نیز آمریکا مدعی بوده است که از سال ۲۰۰۶ به بعد، هیچ تحقیقی بر روی داده‌ها صورت نگرفته است؛ مگر اینکه تحلیلگران در برنامه ردیابی تأمین مالی تروریسم با توجه به اطلاعات قبلی، رابطه‌ای میان موضوع جستجو و تروریسم پیدا کرده باشند^۲.

1. Swift.com/about_swift/company_information/swift_history

2. Aei.pitt.edu/43185/1/LSE_No_56_Dataveillance.pdf

با این حال به گفته استوارت لوی، معاون تروریسم و اطلاعات مالی وزارت خزانه داری «جستجوهای زیادی در پایگاه داده‌های سوئیفت صورت گرفته است. من تعداد دقیق آنها را نمی‌دانم، ولی می‌دانم که حداقل ده ها یا صدها هزار جستجو صورت گرفته است»^۱. همچنین به گفته جان اسنو وزیر وقت خزانه‌داری آمریکا، سوئیفت در پاسخ به احضاریه‌های اداری گفته بود که قادر نیست جستجوهای جداگانه از اطلاعات را بدهد و لذا تمام سوابق معاملات را به آمریکا ارائه داده است.^۲

این توضیحات نشان می‌دهد که از آنجایی که امکان جستجو در بخش خاصی از داده‌های سوئیفت وجود نداشته است، لذا سطح دسترسی آمریکا به داده‌های سوئیفت، محدودیت نداشته و تمامی مبادلات را شامل می‌شده است؛ مسئله‌ای که باعث شکایت گسترده کشورها به ویژه کشورهای اروپایی گردید.

1. [Privacyinternational.org/node/534](https://www.privacyinternational.org/node/534)

بخش چهارم

شکایت کشورها از سوئیفت به دلیل جاسوسی آمریکا

برنامه مخفی بین دولت وقت آمریکا و شرکت تعاونی سوئیفت جهت دستیابی به اطلاعات مالی کشورها، در ژوئن ۲۰۰۶ توسط روزنامه‌های آمریکا در گزارش دقیقی به طور کامل افشا شد. این افشاگری، موجب اختلاف بین اتحادیه اروپا و آمریکا و شکایت متعدد کشورها علیه سوئیفت و آمریکا به دلیل عدم رعایت حقوق خصوصی افراد گردید. علاوه بر این، پس از انتشار اطلاعات مربوط به همکاری سوئیفت با آمریکا، شرکت تعاونی سوئیفت به دلیل عدم احترام به قوانین حریم خصوصی، با بدبینی سایر کشورها مواجه شد. مسئله‌ای که بعدها تبدیل به انگیزه‌ای برای کشورها جهت طراحی و راه‌اندازی سامانه‌های موازی برای این پیام‌رسان شد.^۱

اختلافات داخلی در آمریکا به دلیل جاسوسی از سوئیفت

افشای ترتیبات میان دولت آمریکا و سوئیفت در جاسوسی از داده‌های مالی افراد، کشمکش‌های داخلی میان کنگره و دولت آمریکا را نیز برجسته کرد. همچنین اثربخشی و قانونی بودن روش‌های دولت در استفاده از این داده‌ها را زیر سؤال برد.

تا زمانی که اقدامات سوئیفت به عنوان بخشی از برنامه ردیابی تأمین مالی تروریسم توسط روزنامه‌ها در ماه ژوئن ۲۰۰۶ منتشر نشده بود، تنها برخی از اعضای کنگره در مورد رابطه بین سوئیفت و وزارت خزانه‌داری آمریکا اطلاع داشتند. با این حال با اشاره به الزامات قانون اختیارات اقتصادی بین المللی رئیس‌جمهور آمریکا، دیگر اعضای کنگره نیز همانند بسیاری از اروپایی‌ها احساس کردند که به اندازه کافی در مورد روش‌هایی که توسط آن داده‌های مالی بدست آمده، نمی‌دانند. علاوه بر این، اعضای کنگره در مورد اینکه آیا برنامه ردیابی تأمین مالی تروریسم از لحاظ قانونی از اعتبار

برخوردار است نیز دچار تفرقه بودند؛ بویژه در این خصوص که آیا برنامه سوئیفت حریم خصوصی شهروندان آمریکایی را نقض می‌کند یا نه.

به لحاظ تاریخی، قانون اساسی آمریکا هیچگونه حفاظتی از اطلاعات مالی اشخاص ثالث در برابر دسترسی دولت فراهم نمی‌کند. برای پوشش این مسئله، کنگره قانون حفاظت از حقوق خصوصی مالی افراد را در سال ۱۹۷۸ تصویب کرده بود که بعضی از افراد را از دسترسی دولت به اطلاعات مالی‌شان محافظت می‌کرد. این قانون دولت را موظف می‌نماید زمانی که به دنبال دسترسی به اطلاعات مالی اشخاص است، از قبل به آنها اطلاع‌رسانی کند. علاوه بر اطلاع‌رسانی به افراد، مقامات باید داده‌های مالی را از مؤسسات بوسیله روش معمول قضایی دریافت کنند.

اما به زعم دولتمردان آمریکایی، این اقدامات، مربوط به مؤسسات سپرده‌گذاری از قبیل بانک‌ها بوده است؛ لذا از آنجایی که سوئیفت یک تعاونی بانکی محسوب می‌شود نه یک بانک، آنها در پاسخ به اعتراضات بیان کردند که نیازی به حمایت از حریم خصوصی افراد نبوده است. بنابراین، یکی از مزایای اصلی احضاریه‌های اداری این بود که مقامات مجبور نبودند احضاریه اداری به بانک‌ها بدهند و یا اینکه فرد مورد نظر را از بررسی اطلاعاتش مطلع نمایند. البته این تحلیل ظاهری دولت آمریکا از قانون بود؛ چرا که حتی مقامات عالی‌رتبه وزارت خزانه‌داری آمریکا اعتراف کردند که استفاده گسترده از احضاریه‌های اداری برای ورود به حریم خصوصی و داده‌های مالی محرمانه افراد از طریق سوئیفت توسط دولت آمریکا، قبلاً سابقه نداشته است.

با این وجود، بلافاصله بعد از افشای استفاده از داده‌های سوئیفت در ژوئن ۲۰۰۶، مجلس نمایندگان حمایت خود را از برنامه ردیابی تأمین مالی تروریسم با تصویب قطعنامه ۸۹۵ نشان داد؛ هرچند مدتی بعد از آن، برخی اعضای کنگره که از احتمال نقض حریم خصوصی افراد نگران بودند، دستورالعمل تحقیق درباره برنامه ردیابی

تأمین مالی تروریسم را صادر کردند که نتیجه آن هنوز هم منتشر نشده است.^۱ در واقع اگرچه به نظر می‌رسد که یک نگرانی دائمی در مورد قانونی بودن برنامه سوئیفت و اینکه آیا قوانین حفظ حریم شخصی افراد نقض می‌شود، در داخل آمریکا نیز وجود داشته است، اما مقامات دولتی آمریکا بر این باور بوده‌اند که این برنامه یک ابزار ضروری برای جنگ علیه تروریسم و کشورهای غیرهمسو است.^۲ به همین منظور، در استفاده حداکثری از آن هیچگونه مانعی ایجاد نکردند.

ایجاد اختلاف میان آمریکا و اروپا به دلیل جاسوسی از سوئیفت

کشورهای اروپایی پس از اطلاع از جاسوسی آمریکا، اعتراضات و مخالفت‌های خود با این اقدام را مطرح کردند. مخالفت دولت‌های اتحادیه اروپا با جاسوسی آمریکا از سوئیفت تحت پوشش برنامه ردیابی تأمین مالی تروریسم، ناشی از دو دلیل بود:

یک) مقامات بالای دولتی اتحادیه اروپا از برنامه بهره‌برداری از داده‌های سوئیفت تا ماه ژوئن ۲۰۰۶ که روزنامه‌های آمریکایی این قضیه را افشاء کنند، آگاه نبودند.

دو) با توجه به نظر مقامات اروپایی، برنامه استفاده از داده‌های سوئیفت، قوانین اروپایی مربوط به حریم خصوصی را نقض می‌کرد.

گزارش پارلمان اروپا، آنچه دیگر کشورهای اروپایی و سازمان‌های دولتی درباره برنامه سوئیفت گفتند را تکرار می‌کرد. این گزارش مربوط به نقض مقررات مختلف حفاظت از اطلاعات اتحادیه اروپا، به خصوص مواردی بود که اطلاعات اشخاص حقیقی را شامل می‌شود. هرچند دولت و مقامات اتحادیه اروپا از نقض قوانین حریم خصوصی افراد نگران بودند، اما حقیقت ناراحتی آنها به واقعیت ساده‌ای بر می‌گشت؛ آن حقیقت این بود که آنها تا مدت‌ها از این وضعیت آگاه نبودند. بنابراین اتحادیه اروپا از آمریکا درخواست کرد که راهی برای تطبیق این برنامه با قوانین خود پیدا کند. به عبارت دیگر

1. Scholarship.law.unc.edu/ncbi/vol11/iss1/16/

2. Privacyinternational.org/node/534

دولت‌های اتحادیه اروپا خواهان توافق مشخص در مورد چگونگی استفاده از داده‌های سوئیفت برای مبارزه با تروریسم بودند؛ در عین حال که این کشورها به دنبال آن بودند که «حقوق افراد اروپایی» نیز حفظ شود.

در این زمینه مقامات آلمان برای حفظ حریم خصوصی افراد سه راه حل ممکن را پیشنهاد دادند. اول اینکه سوئیفت تمام سرورهای داده خود را به کشورهای اروپایی و خارج از آمریکا منتقل کند. دوم اینکه یک سطح بالاتری از رمزگذاری بر روی اطلاعات مالی انجام شود، به طوری که مقامات آمریکایی امکان مشاهده اطلاعات را نداشته باشند. سوم اینکه تمام بانک‌ها به مشتریان خود اطلاع دهند که در سامانه فعلی، اطلاعات مالی آنها ممکن است امن نباشد. هر چند این سه راه حل قابل قبول به نظر می‌رسیدند، اما هیچ‌گاه اجرایی نشدند و مقامات آلمانی نیز امیدی به اجرای آن نداشتند.^۱ در واقع در حالی که کشورهای عضو اتحادیه اروپا منتقد برنامه سوئیفت و دسترسی آمریکا به آن بودند، اما این واقعیت که آنها پیگیر این مسئله نبوده‌اند یا قصد نداشتند اقدامات قانونی علیه سوئیفت یا آمریکا را دنبال کنند، مؤید این ادعاست که مقامات آمریکایی همچنان به ارائه احضاریه‌های اداری به تعاونی سوئیفت و دریافت اطلاعات مدنظر خود از آن ادامه داده و خواهند داد و سوئیفت نیز با این کشور همکاری کرده است.^۲

شکایت ۳۲ کشور و چند نهاد بین‌المللی از آمریکا به دلیل جاسوسی از سوئیفت

گزارش‌هایی از متصدی حفاظت اطلاعات ملی بلژیک و مقامات حفظ حریم خصوصی آلمان، سوئیفت را متهم به نقض قوانین حریم خصوصی اروپا می‌دانستند. اما سوئیفت در موضع خود باقی ماند و ارائه اطلاعات مالی به آمریکا را طبق قوانین آمریکایی و اروپایی لازم الاجرا دانست. علاوه بر این، سوئیفت خاطرنشان کرد که مکرراً اطمینان

1. Scholarship.law.unc.edu/ncbi/vol11/iss1/16/

2. Aei.pitt.edu/43185/1/LSE_No_56_Dataveillance.pdf

خود را از آمریکا دریافت کرده که اطلاعات مالی ارائه شده اشخاص، تنها در تحقیقات تروریستی مورد استفاده قرار گیرد و در محیط امن محافظت شود. با این حال، این توضیحات از نظر دولت‌های اروپایی کافی نبوده و این اقدام سوئیفت غیرقانونی بوده است.

مؤسسه حریم خصوصی بین‌المللی در ماه جولای ۲۰۰۶ شکایات متعددی را از طرف مقامات ژاپن، کره جنوبی، تایوان، چین، تایلند و آرژانتین در رابطه با برنامه سوئیفت دریافت کرد. این شکایات مربوط به حفاظت از اطلاعات و حریم خصوصی کشورها بود که از طرف ۳۲ کشور، به دلیل آشکارسازی و افشای اطلاعات محرمانه پایگاه داده‌های سوئیفت به مقامات و سازمان‌های آمریکایی، انجام شد. در این شکایات، کشورها از این بابت که داده‌های سوئیفت توسط مقامات آمریکایی برای طیف وسیعی از فعالیت‌های غیرمرتبط از جمله جاسوسی مورد استفاده قرار گیرد، ابراز نگرانی کردند؛ داده‌هایی که اطلاعات کاربران سوئیفت در سراسر جهان را شامل می‌شد.^۱ تمامی این شکایات، حاکی از آن بود که دسترسی آمریکا به سوئیفت، بدون در نظر گرفتن روند قانونی حفظ حریم خصوصی انجام شده و هیچ مبنای قانونی معتبری نداشته است.

در ادامه این شکایات کشورها، موسسه حریم خصوصی بین‌المللی به تعاونی سوئیفت هشدار داد که رسوایی به بار آمده باعث ایجاد بی‌اعتمادی شدید در امنیت نظام بانکداری بین‌المللی می‌شود. سیمون داویس مدیر بین‌المللی موسسه حریم خصوصی گفته بود که «سوئیفت هیچ توجهی به نگرانی‌های عمومی بانک‌ها و مشتریان نکرده است. یک تهدید واقعی در این محیط حساس وجود دارد که هم آسیا و هم جهان غرب به سمت ایجاد نظامات (پیام‌رسان مالی) مخصوص خود حرکت کنند».^۲ سوئیفت در مدتی که این شکایات و اعتراضات مطرح شد، همچنان ساکت بود و فقط یک بیانیه

1. Privacyinternational.org/node/534

در سایت خود منتشر کرد که بر اساس آن، اعلام شد این نهاد هیچ اطلاعات معناداری را افشا نکرده است. به گفته سیمون داویس، این خیلی عجیب است که سوئیفت این اتهامات سنگین را قبول نکرد؛ مقیاس عملیات سوئیفت بسیار نفس گیر و میزان نقض حریم خصوصی بی سابقه است.^۱

بر اساس گزارشات سالانه سوئیفت و گفتگوهای انجام شده با مسئولین این نهاد، موسسه حریم خصوصی بین المللی تخمین زده است که تقریباً یک درصد از ۲ میلیارد معاملات سالانه سوئیفت یعنی ۲۰ میلیون پرونده فقط در سال ۲۰۰۴-۲۰۰۵ به طور مخفیانه به آمریکا منتقل شده است. پس از این شکایات، نه دولت آمریکا و نه تعاونی سوئیفت آماده ارائه جزئیات درباره میزان افشای اطلاعات نشدند. با این حال دفتر نخست وزیر بلژیک تأیید کرد که این تعاونی، احضاریه‌های اداری گسترده‌ای برای دریافت میلیون‌ها پرونده دریافت کرده است. علاوه بر این، بسیاری از گروه‌های حقوق بشری نیز، شکایاتی را علیه سوئیفت انجام دادند. این عده در مقابل ادعای مقامات آمریکا مبنی بر ردیابی تأمین مالی تروریسم از طریق سوئیفت، پاسخ دادند که تروریست‌ها مطلع هستند که امکان ردیابی مالی‌شان وجود دارد و بنابراین ردیابی این اطلاعات، فایده‌ای در مبارزه با تروریسم ندارد. لذا احتمال استفاده از داده‌های مالی اشخاص توسط آمریکا برای اهدافی غیر از ردیابی تروریسم وجود دارد.^۲

۱. همان

۲. همان

بخش پنجم

جاسوسی مشترک پس از تفکیک سوئیفت میان اروپا و آمریکا

نمایندگان تعاونی سوئیفت به دلیل قرارداد مالی اتحادیه اروپا در اختیار آمریکا، از جانب این اتحادیه تحت فشار بودند. در نتیجه در سال ۲۰۰۹ سوئیفت معماری فنی خدمات پیام رسانی خود را که بر اساس سرورهای آینه‌ای در هلند و ایالات متحده قرار داشت، تغییر داد. این اصلاحات شامل ایجاد مراکز عملیاتی جدید در سوئیس جهت حفظ پیام‌های مالی مربوط به اتحادیه اروپا بود؛ به عبارت دیگر نمایندگان سوئیفت در نظر داشتند که پیام‌های سوئیفت اروپا را در سرورهای آینه‌ای در هلند و سوئیس ذخیره‌سازی نمایند و از ذخیره داده‌های اروپایی در سرورهای آمریکایی جلوگیری کنند.^۱

برای انجام این کار، آنها پلتفرم پیام‌رسانی بین‌المللی خود را به دو ناحیه جداگانه تقسیم بندی کردند. این معماری توزیع شده، عملیات پیام‌رسانی را به دو منطقه پیام رسانی اروپایی و آمریکایی^۲ تقسیم کرد. در این تقسیم بندی، پیام‌های اروپایی در دو قسمت هلند و بخشی از مرکز عملیاتی سوئیس ذخیره‌سازی می‌شد. پیام‌های منطقه‌ای آتلانتیک نیز در آمریکا و بخشی از مراکز عملیات سوئیس ذخیره سازی می‌گردید و از پیام‌های منطقه اروپا جدا شد.

کشورهای خارج از اروپا به طور پیش فرض به منطقه آتلانتیک (آمریکایی) اختصاص داده شدند؛ اما می‌توانستند پیام‌های خود را در منطقه اروپا نیز ذخیره سازی کنند. به عبارتی دیگر، منطقه اروپایی اطلاعات مربوط به پیام‌رسانی ناحیه اقتصادی اتحادیه اروپا (یورو ۲۷، نروژ، ایسلند و لیختن اشتاین) و سایر قلمروهای وابسته به اروپا

1. Aei.pitt.edu/43185/1/LSE_No_56_Dataveillance.pdf

۲. منظور از آمریکا، منطقه تحت نظر آمریکا یعنی آن سوی اقیانوس اطلس (منطقه آتلانتیک) است.

را پوشش می‌داد. منطقه پیام‌رسانی آتلانتیک نیز شامل آمریکا و نواحی وابسته به آن و همچنین سایر ۱۸۰ کشور جهان می‌شد که به طور پیش فرض به منطقه آتلانتیک واگذار شده بودند.

بر اساس دسته‌بندی جدید، مقامات دفتر کنترل دارایی‌های خارجی وزارت خزانه‌داری آمریکا (اوفک)، دیگر نمی‌توانستند درخواست دسترسی به پیام‌های بین بانکی که در اروپا تبادل می‌شد را داشته باشند و برنامه ردیابی تأمین مالی تروریسم آمریکا، تنها به داده‌های سوئیت ذخیره شده در ناحیه آتلانتیک دسترسی داشت.^۱

دسترسی مجدد آمریکا به داده‌های سوئیت اروپایی

به دنبال این بازمعماری، در سال ۲۰۰۹ آمریکا مذاکرات غیر رسمی آتلانتیک را با اتحادیه اروپا شروع کرد تا بتواند به داده‌های سوئیت اروپایی نیز دسترسی پیدا کند. این اقدام از سوی مقامات حفاظت اطلاعات اتحادیه اروپا و بسیاری از افراد دیگر مورد انتقاد قرار گرفت. با این حال در دور دوم مذاکرات، جهت اصلاح موارد و ایرادات مطرح شده، دو عنصر مهم به توافقنامه افزوده شد. اول مقرر گردید تا یک سرپرست از طرف اتحادیه اروپا در آمریکا به عنوان یک حفاظت اضافی، بر استفاده آمریکا از داده‌ها نظارت کند. هدف از این اقدام، اطمینان از آن بود که داده‌ها مستقیماً در راستای ردیابی مالی تروریسم استفاده شود. دوم هم اینکه آژانس اجرای قانون اتحادیه اروپا (یورپل)، به عنوان سازمان مشترک، برای نظارت بر درخواست‌های رسمی اوفک جهت استفاده از داده‌های مالی سوئیت اروپایی تعیین شد. بر این اساس، علیرغم اینکه اروپا با تقسیم سوئیت به دو بخش، تلاش کرده بود تا اطلاعات مالی کشورهای تحت پوشش خود را از نظارت آمریکا خارج کند، اما دسترسی دوباره این کشور از طریق سازوکار ایجاد شده مجدداً فراهم گردید.^۲

۱. همان

۲. همان

انتقال انبوه داده‌های سوئیفت اروپایی به آمریکا، یکی از دلایل اصلی نمایندگان پارلمان اروپا و نمایندگان ادارات حفاظت اطلاعات اروپا شده بود تا چارچوب قانونی و فنی مناسب برای استخراج داده‌های مورد نیاز جهت ردیابی مالی تروریسم را ایجاد کنند؛ تا بدین طریق، مانع جاسوسی آمریکا از اطلاعات مالی منطقه خود شوند. لذا نمایندگان در تلاشی مجدد جهت جلوگیری از انتقال انبوه داده‌ها به آمریکا، اقدام به ایجاد یک برنامه اروپایی معادل برنامه ردیابی تأمین مالی تروریسم آمریکا نمودند.

طبق این برنامه، اروپا در جولای ۲۰۱۱ یک «سامانه ردیابی مالی تروریسم اروپایی»^۱ راه‌اندازی کرد که به دنبال هدفمند کردن انتقال اطلاعات سوئیفت به آمریکا بود. با ایجاد این سامانه، اروپا به دنبال تحلیل مالی داده‌های تروریسم در قلمرو خود بود. پیش از این، آمریکا داده‌ها را به شکل انبوه دریافت می‌نمود و با استفاده از برنامه ردیابی تأمین مالی تروریسم خود، به جستجو در داده‌ها می‌پرداخت. حال با ایجاد این سامانه، فقط داده‌های مربوط به تروریسم، آن هم توسط اروپا شناسایی و سپس در اختیار آمریکا قرار می‌گرفت.

با این حال، برخی سامانه ردیابی مالی تروریسم اروپایی را برنامه حفاظت از داده‌ها قلمداد نمی‌کردند، بلکه آن را به عنوان توسعه همکاری‌های بیشتر با آمریکا توصیف می‌نمودند که بهره‌برداری از داده‌های مالی اشخاص در پایگاه داده‌های سوئیفت را از طریق شیوه‌های امنیتی و اطلاعاتی توجیه می‌کرد. در این روش جدید، اتحادیه اروپا (به جای آمریکا) درخواست دریافت اطلاعات را به تعاونی سوئیفت ارسال می‌کرد. سپس اطلاعات مالی بدست آمده را در یک پایگاه داده جدید مستقر در اتحادیه اروپا جمع‌آوری نموده و سرانجام یک جستجوی هدفمند انجام می‌داد و نتیجه حاصل از آن را تجزیه و تحلیل و به آمریکا ارسال می‌کرد. در نتیجه هر چند در راستای حفاظت از داده‌ها، نمایندگان پارلمان اروپا یک رویکرد دو مرحله‌ای اتخاذ نمودند تا داده‌های انبوه مستقیماً در دسترس آمریکا قرار نگیرد، اما در واقع آنها با این اقدام خواستار تقلید

برنامه‌های آمریکا شدند؛ برنامه‌هایی که قبلاً مورد انتقاد اروپا و سایر کشورها قرار گرفته بود.

استمرار جاسوسی از سوئیفت

بعد از نارضایتی اتحادیه اروپا نسبت به جاسوسی آمریکا از داده‌های سوئیفت، بازمعماری این نهاد سبب ایجاد یک توازن دوباره در روابط قدرت میان اروپا و آمریکا شد. با این حال، وضعیت در مورد کشورهای ثالث (غیر از آمریکا و اتحادیه اروپا) و شهروندانشان در سراسر جهان تغییری نکرد. در واقع داده‌های تعاونی سوئیفت که متعلق به بیش از ۲۲۰ کشور در سراسر جهان است، همچنان از طریق سوئیفت توسط اروپا و آمریکا مورد بهره‌برداری قرار می‌گیرد و قوانین حفاظت از حریم خصوصی افراد همچنان نقض می‌شود.^۱ هکرها در آپریل ۲۰۱۷ نیز اسنادی را منتشر کردند که طبق آن مشخص شده است آژانس امنیت ملی آمریکا هنوز به پیام‌رسان بین بانکی سوئیفت دسترسی داشته و به این ترتیب توانسته بر جریان پولی میان بانک‌های خاورمیانه و آمریکای لاتین نظارت کند.^۲

1. Aei.pitt.edu/43185/1/LSE_No_56_Dataveillance.pdf

2. Heinonline.org/HOL/LandingPage?handle=hein.journals/jhtl8&div=7&id=&page=

بخش نهم

کارکردهای سوئیفت برای آمریکا

شواهد و قرائنی که در بخش‌های قبل ارائه گردید، نشان داد که سامانه پرداخت و انتقال وجه بین‌المللی سوئیفت، علیرغم ماهیت و آنچه مسئولین آن می‌گویند، تحت اختیار و نظارت آمریکا قرار دارد. تمرکز این اختیارات، موقعیتی را برای آمریکا به وجود آورده است که می‌تواند از طریق آن، فعالیت‌ها و اطلاعات مربوط به نقل و انتقالات مالی بین‌المللی کشورها را در راستای اهداف خود رصد کرده و محدودیت‌هایی از قبیل تحریم، بر سر راه کشورها ایجاد نماید.

ابزار جاسوسی از اطلاعات مالی کشورها

آری پائول، یک افسر ارشد اطلاعاتی آمریکا در این زمینه گفته است: سوئیفت یک شبکه مالی است که از طریق دلار آمریکا، به فرآیند انتقال وجه بین بانکی کمک می‌کند و کاملاً واضح است که این سامانه انتقالات مالی، به عنوان بخش نظامی وزارت خزانه داری آمریکا عمل می‌نماید. وی افزوده است: یک مسئله دیگری که امروزه شکل گرفته، بحث ایجاد محرومیت مالی است. به عبارت ساده تر یک دولت یا بانک، اقداماتی را در پیش می‌گیرد که یک کشور یا گروهی از مردم را از دسترسی به خدمات مالی محروم کند. این اقدامات در رابطه با سوئیفت به وضوح صادق است. سوئیفت یک میراث بین‌المللی باقی مانده برای آمریکا است که برای انتقال پیام مالی بین بانک‌ها طراحی شده است!

به گفته آری پائول، دولت‌های آمریکا از سوئیفت به عنوان وسیله‌ای برای اعمال فشار به گروه‌ها و کشورهای مختلف استفاده می‌کنند. اولین نمونه از این اقدام به سال ۲۰۰۰ بر می‌گردد که در آن داده‌های کاربران مختلفی از جهان جمع‌آوری و استفاده شد. این اقدامات آمریکا ترکیبی از قدرت سخت و نرم است که به طور مخفیانه داده‌های افراد مختلف را برای چندین سال متوالی از سوئیفت جمع‌آوری نموده است. هنگامی که این ماجرا علنی

شد، آمریکا برای ادامه دسترسی خود به شیوه هک کردن و انتقال داده‌ها متوسل گردید.^۱

ابزار تحریم کشورهای غیرهمسو

علاوه بر کسب اطلاعات، ایجاد محدودیت در دسترسی به سوئیفت نیز به عنوان ابزار جنگ اقتصادی در اختیار آمریکا قرار دارد. به گفته آری پائول، تنها دلیل اینکه سوئیفت تاکنون بدین شکل منسوخ و قدیمی مانده، این است که آمریکا نیاز به آن دارد تا کشورها را تهدید کرده یا دچار محرومیت کند و اگر کشورها یک سامانه مالی جدید ایجاد می‌کردند، در آن صورت دیگر آمریکا چنین کنترلی را از دست می‌داد. وی افزوده است: از بزرگترین معایب سامانه‌های متمرکز در دنیا این است که پیوستن به آن نیاز به اجازه دارد و این، محرومیت مالی را نیز به دنبال خواهد داشت؛ در واقع کسی که بر این سامانه‌ها سلطه دارد، متعصبانه عمل خواهد کرد. بنابراین تسلط آمریکا بر سوئیفت به این دلیل بسیار خطرناک است.^۲

جیمز ریکاردز مشاور تهدیدات مالی و جنگ نامتقارن «سازمان اطلاعات مرکزی آمریکا»^۳ و نویسنده کتاب جنگ‌های ارزی که نقش پررنگی در طراحی و اعمال تحریم‌های مالی و بانکی علیه ایران داشته نیز در اهمیت سوئیفت گفته است: آمریکا نه تنها دلار را کنترل می‌کند، بلکه سامانه‌های پرداختی آن را نیز تحت کنترل خود دارد. این کنترل‌ها شامل سرشماری دیجیتالی خزانه‌داری از دارندگان بدهی‌های دلاری بوسیله «ابزارهای تسویه فدوایر»^۴ در بانک‌های عضو و «اتاق‌های پایاپای و تسویه»^۵ که ترکیبی از بانک‌های بزرگ آمریکایی است، می‌شود. پرداخت حتی یک دلار از بانک شانگهای چین به بانک سیدنی استرالیا اگر از طریق سوئیفت انجام شود، به اطلاع وزارت خزانه‌داری آمریکا می‌رسد.^۶

۱. همان

۲. همان

3. Central Intelligence Agency (CIA)

4. Fedwire Settlement System

5. Clearing House Interbank Payment System

6. <https://dailyreckoning.com/the-u-s-dollar-a-victim-of-its-own-success/>

بخش هفتم

آسیب‌های سوئیفت برای اقتصاد ایران

جمهوری اسلامی ایران یکی از کشورهایی است که همواره از جانب آمریکا، به اقدامات تروریستی متهم شده است؛ لذا یکی از اطلاعاتی که در سوئیفت به صورت مستمر تحت رصد آمریکا قرار داشته، اطلاعات مرتبط با مبادلات مالی ایران بوده است. این مسئله منجر به این شد که جریان مالی کشور شناسایی شود و به راحتی تحت تحریم قرار گیرد.

شناسایی اطلاعات ایران با سوئیفت و قطع دسترسی در سال ۱۳۹۰

پیش از سال ۱۳۹۰ و دوره اول تحریم‌ها، سوئیفت به آمریکا کمک کرد تا این کشور بتواند تمام جریان مالی ایران را شناسایی کند؛ سپس ایران را از مسیرهای شناسایی شده تحریم نماید و با قطع دسترسی به سوئیفت، زمینه را برای قفل کردن مبادلات مالی کشور فراهم کند.

با بالا گرفتن اختلاف نظرهای بین‌المللی در خصوص مسائل هسته‌ای کشور و در راستای وضع تحریم‌های مالی توسط آمریکا، در روز شنبه ۲۷ اسفند ۱۳۹۰ در پایان ساعت اداری رسمی کشور، دسترسی بانک مرکزی ایران به سوئیفت قطع شد. بانک‌های هدف در قطع دسترسی به سوئیفت شامل بانک صادرات، بانک ملت، پست بانک و بانک سپه بودند. به دنبال تفاهم میان ۲۷ کشور اتحادیه اروپا و حکم صادره بر اساس آن، سوئیفت همه بانک‌های ایرانی را از شبکه بین‌المللی خود حذف کرد.

هر چند تحریم سوئیفت، مرادوات بین‌المللی بانک‌های ایرانی را متوقف نکرد، اما هزینه‌های زیادی بر عملیات ارزی و بانکی کشور تحمیل نمود. این اقدام نشان داد که کشورهای اروپایی و آمریکا که سکنداران اصلی سوئیفت هستند، نه تنها از داده‌های

سوئیفت به نفع خود و علیه کشورها استفاده می‌کند، بلکه با سوءاستفاده از این ابزار، کشورها را از طریق آن تحت تحریم‌های بانکی قرار می‌دهند.

بازگشت مجدد به سوئیفت و قطع دسترسی در سال ۱۳۹۷

با دستیابی به توافق هسته‌ای موسوم به برجام بین ایران و کشورهای گروه ۱+۵ در تاریخ ۲۷ دی ۱۳۹۴ و اجرای آن، تحریم سوئیفت از ایران برداشته شد. پس از لغو این تحریم، بانک‌های تجارت، رفاه کارگران، توسعه صادرات، سپه، پست بانک، صنعت و معدن، بانک ایران و اروپا، بانک توسعه تعاون، سینا، ملت و ملی به سوئیفت متصل شدند؛ بانک مرکزی نیز به دنبال افزایش به کارگیری سوئیفت توسط بانک‌های ایرانی بود و آمار پیام‌های رد و بدل شده در این پیام‌رسان را به عنوان یک دستاورد ارائه می‌نمود. با بازگشت دوباره ایران به سوئیفت، مجدداً این امکان در اختیار آمریکا قرار گرفت که مبادلات مالی و مسیرهای جدید کشور را رصد نماید. این اقدام نیز در نهایت به تحریم‌های سال ۱۳۹۷ و تهدید ایران به اخراج از سوئیفت و قطع دسترسی کشور به این پیام‌رسان منجر شد و ضربه ای دیگر از سوئیفت به کشور وارد گردید.

استفاده دو وجهی آمریکا از سوئیفت علیه ایران

آمریکا از ابزار سوئیفت به دو شکل علیه ایران استفاده نموده است. شکل اول، رصد مبادلات ایران است؛ دولت آمریکا با دسترسی غیرقانونی که به سوئیفت و داده‌های آن دارد، این امکان را دارد تا همه مبادلات انجام شده در آن را رصد نماید و از وضعیت کشورهای مدنظر خود از جمله ایران، در مبادلات جهانی شان اطلاع یابد. شکل دوم، تهدید ایران به قطع سوئیفت است که منجر به ایجاد اختلال در مبادلات بانکی کشور می‌شود. در واقع از آنجا که پیام‌رسانی مبادلات مالی ایران از طریق سوئیفت انجام می‌شود، قطع این دسترسی، ایران را در انجام تجارت با کشورها و فرآیندهای مالی آن با مشکل مواجه می‌کند.

با این وجود، جالب توجه است که قبل از اعمال تحریم‌ها، علاوه بر عملیات مالی بین‌المللی، عملیات بانک‌های داخلی ایران با یکدیگر نیز توسط سوئیفت صورت می‌گرفته است. اما با اعمال تحریم‌ها، نظام بانکی داخلی دچار مشکل شد و جهت رفع مشکل، در تیرماه سال ۱۳۹۱ سامانه داخلی سپام (سامانه پیام‌رسان الکترونیکی مالی) به منظور انجام فعالیت‌های بانکی داخلی طراحی گردید؛ سامانه‌ای که می‌توانست به مبادلات خارجی ایران نیز تسری یابد. اما استفاده از سامانه سپام توسعه نیافت و بعد از انعقاد قرارداد برجام و با وجود تجربیات و ضربات زیادی که از سوئیفت بر کشور وارد شد، بانک‌های ایرانی با پیگیری بانک مرکزی مجدداً به سوئیفت بازگشتند.

بخش هشتم

گسترش پیام‌رسان‌های موازی سوئیفت در جهان و واکنش آمریکا

پس از افشای دسترسی بی حد و حصر آمریکا به سوئیفت و مشخص شدن آثار منفی همکاری با این پیام‌رسان، کشورها به تدریج مسیرهای جدیدی را باز نمودند تا رفته رفته وابستگی خود به این زیرساخت مالی را کاهش دهند. در حال حاضر بسیاری از کشورها جهت رهایی از هزینه و ریسک ناشی از مبادلات دلاری و همچنین نقل و انتقالات سوئیفت و حذف نقش بانک‌ها و مراحل واسط اضافی، اقدام به استفاده از پیام‌رسان‌های موازی با سوئیفت نموده‌اند. در این زمینه چین و روسیه پیشتاز بوده و دیگر کشورها نیز رفته رفته در حال ایجاد پیام‌رسان‌های موازی سوئیفت هستند.

پیام‌رسان موازی سوئیفت در چین

به عنوان نمونه‌ای از این پیشرفت‌ها در حوزه پیام‌رسان مالی می‌توان به «سامانه پرداخت بین بانکی بین‌المللی چین»^۱ یا شبکه مالی پرداخت‌های چین اشاره کرد که به منظور بهره‌برداری در پرداخت‌های بین بانکی مورد استفاده قرار می‌گیرد. این سامانه درگاهی برای پرداخت و تسویه معاملات است که توسط بانک مرکزی چین به عنوان موازی برای سوئیفت راه اندازی شده است. هدف از راه‌اندازی این سامانه ارائه خدمات ایمن، آسان و کارآمد به مؤسسات مالی بین‌المللی و بانک‌های فراساحلی چینی جهت انجام معاملات مبتنی بر یوآن بوده است. فراگیر شدن این شبکه مالی می‌تواند پیامدهای متعددی را برای سوئیفت داشته باشد.

کشور چین از سال ۲۰۱۵ در راستای افزایش استفاده از یوآن در معاملات بین‌المللی، اقدام به راه‌اندازی سامانه پرداخت بین بانکی بین‌المللی (CIPS) نموده است. هدف از راه‌اندازی این سامانه پرداخت، کاهش وابستگی به سامانه پرداخت دلاری آمریکا در

1. Cross-Border Interbank Payment System (CIPS)

معاملات میان چین با کشورهای طرف تجاری است.

سامانه پرداخت بین بانکی بین‌المللی چین، بدون نیاز به استفاده از سامانه‌های پرداختی غرب و با تسهیل مبادلات مالی میان کشورهای مختلف، کل شبکه مبادلات فرامرزی پرداخت شده توسط یوآن در تجارت با تمام شرکای چین را پوشش می‌دهد. کشور چین در این پرداخت‌ها یکی از طرفین مبادلات است.

طبق گزارش منتشره شده توسط سامانه پرداخت بین بانکی بین‌المللی چین، تا پایان ماه می ۲۰۱۷، استفاده‌کنندگان مستقیم از سامانه پرداخت بین بانکی بین‌المللی چین با میزان پرداخت‌های بالا، به تعداد ۲۸ کاربر رسیده بود. همچنین تعداد استفاده‌کنندگان غیرمستقیم از این سامانه نیز به ۵۷۴ کاربر رسیده است.

این سامانه از زمان راه‌اندازی تاکنون با تقاضای فزاینده‌ای جهت استفاده مواجه بوده است. در سال ۲۰۱۷ حجم معاملاتی که از طریق CIPS پردازش شده است، نسبت به سال گذشته، تقریباً دو برابر شده است و به عدد ۱.۲۶ میلیون تراکنش رسیده است. همچنین ارزش کل معاملات انجام شده توسط CIPS در سال ۲۰۱۷ نسبت به سال قبل، رشد ۲۳۴ درصدی داشته است و به عدد ۱۴.۵۵ هزار میلیارد یوآن رسیده است.

در فوریه سال ۲۰۱۹، ۶ مؤسسه مالی به عنوان کاربر دارای دسترسی غیرمستقیم، به CIPS پیوسته‌اند. از میان این ۶ کاربر، ۳ کاربر در سرزمین اصلی چین و ۳ کاربر نیز در بیرون از سرزمین اصلی قرار دارند. در حال حاضر ۳۱ بانک، کاربر مستقیم CIPS هستند. همچنین تا جولای ۲۰۱۹، کل کاربران غیر مستقیم CIPS به ۸۴۷ عدد رسیده است که از میان آنها ۵۶۰ کاربر در آسیا، ۱۰۵ کاربر در اروپا، ۳۳ کاربر در آفریقا، ۲۵ کاربر در آمریکای شمالی، ۱۸ کاربر در اقیانوسیه و ۱۶ کاربر نیز در آمریکای جنوبی قرار دارند. تا تاریخ مذکور، دسترسی ۸۹ کشور و منطقه به سامانه پرداخت CIPS جهت انجام معاملات یوآنی، توسط این کاربران غیرمستقیم فراهم شده است.^۱ این در حالی

1. Cips.com.cn/cipsen/7052/7057/index.html

است که در زمان راه‌اندازی فاز اول CIPS در اکتبر ۲۰۱۵، در ابتدای کار ۱۹ بانک تجاری در سرزمین اصلی چین به عنوان کاربر دارای دسترسی مستقیم و ۱۷۶ بانک به عنوان کاربر دارای دسترسی غیر مستقیم از بیش از ۵۰ کشور حضور داشتند.

مزیت استفاده از سامانه پرداخت CIPS و یوآن این است که نیازی به زیرساخت‌های پرداختی جدیدی نیست و مؤسسات امکان انتخاب بانک کارگزار مناسب جهت پرداخت‌های خود را دارند؛ همچنین امکان استفاده راحت از یوآن در پرداخت‌ها وجود دارد.

پیام‌رسان موازی سوئیفت در روسیه

از دیگر کشورهای پیشرو در زمینه راه‌اندازی پیام‌رسان مالی موازی سوئیفت، کشور روسیه است. در سال ۲۰۱۴ و زمانی که اتحادیه اروپا و آمریکا اولین دور تحریم‌های بین‌المللی را به دلیل آنچه «مداخله در بحران اوکراین و الحاق کریمه توسط روسیه» خوانده شده بود، علیه مسکو اعمال کردند، این کشور شروع به طراحی یک سامانه پیام‌رسان مالی بین‌المللی^۱ کرد که قرار است جایگزینی برای عملیات سوئیفت در سطح بین‌الملل باشد.

پیام‌رسان مالی بین‌المللی روسیه، هم به لحاظ تکنولوژیک و هم به لحاظ دسترسی به داده‌ها، ویژگی‌های متمایزی نسبت به سوئیفت دارد. به عنوان نمونه با استفاده از این پیام‌رسان، داده‌ها فقط در یک یا دو کشور خاص ذخیره نمی‌شوند، بلکه قرار است در یک شبکه‌ای از کشورها گسترده شود و مراکز متعددی داشته باشد تا از سوء استفاده‌های امنیتی و اطلاعاتی از این داده‌ها به نفع چند کشور خاص جلوگیری شود. همچنین این سامانه پیام‌رسانی منطبق بر استانداردهای معتبر بین‌المللی طراحی شده است؛ این بدین معنی است که در تمامی کشورهای جهان قابلیت استفاده و راه‌اندازی را دارد و توانایی تبادل با سوئیفت را نیز به صورت مستقیم دارد.

1. System for transfer of financial messages (SPFS)

در حال حاضر بیش از ۳۰۰ بانک روسی و همچنین شرکت‌های نفتی و سرمایه‌گذاری متعدد به پیام‌رسان موازی سوئیفت روسیه متصل شده‌اند. روسیه، اعضا و شرکای بریکس را دعوت کرده است تا به این سامانه موازی سوئیفت بپیوندند تا کنترل آمریکا بر نظام مالی بین‌المللی را از بین ببرند.

اخیراً رسانه‌های روسی اعلام کرده‌اند که سامانه موازی سوئیفت روسیه تا سال ۲۰۱۹ بر بستر فناوری بلاک چین فعالیت خود را ادامه خواهد داد. هدف از طراحی سامانه موازی سوئیفت روسیه بر اساس فناوری بلاک‌چین، افزایش امنیت و شفافیت این سامانه و امکان استفاده از آن در زمینه‌ها و موارد مختلف عنوان شده است. در این صورت امکان حذف و سرقت داده‌ها وجود نخواهد داشت و اطلاعات به صورت خودکار برای همه اعضای سامانه با هر تغییر صورت گرفته، به روزرسانی خواهد شد؛ همچنین قرار گرفتن بلاک‌چین به عنوان پشتوانه و بستر سامانه پرداخت بین‌المللی روسیه می‌تواند از هک شدن آن نیز جلوگیری نماید؛ این درحالیست که بانک‌های روسی در استفاده از سوئیفت با این مشکل مواجه هستند^۱.

علاوه بر این، روسیه یک سامانه پرداخت کارتی بنام میر^۲ برای تبادلات مالی طراحی کرده است تا پرداخت‌های خرد داخلی را به عنوان جایگزین سامانه‌های بین‌المللی مانند ویزا و مسترکارت انجام دهد. در حال حاضر ۹۰ درصد دستگاه‌های خودپرداز روسیه به این سامانه پرداخت داخلی متصل هستند که نسخه داخلی ویزا و مسترکارت برای روسیه می‌باشد.

فناوری بلاک چین رقیب جدی سوئیفت

از معماری‌های جدید نرم‌افزاری که برای ایجاد پیام‌رسان مالی موازی سوئیفت استفاده

1. Eurasiareview.com/26032017-russia-creates-alternative-to-swift-banking-payment-system-oped/

2. National payment system (MIR)

می‌شود، فناوری بلاک‌چین است که امکان طراحی پیام‌رسان مالی غیرمتمرکز را فراهم کرده است. اهمیت فناوری بلاک‌چین از زمان آغاز به کار آن مورد توجه متخصصان حوزه‌های فناوری اطلاعات قرار داشت؛ اما در سال ۲۰۱۷ میلادی و با استقبال گسترده از پول‌های الکترونیکی، اهمیت این فناوری توجه بیشتری را به خود جلب نموده است.

فناوری بلاک‌چین^۱ سلسله حساب‌های توزیع شده است که از داده‌های دیجیتالی نامنظم و ثبت شده در بسته‌های بلوک^۲ و در یک زنجیره^۳ خطی استفاده می‌کند؛ این فناوری در راه‌اندازی و پشتیبانی ارزهای دیجیتالی از قبیل بیت‌کوین، اتریوم و دیگر ارزهای رمزنگاری شده نیز مورد استفاده قرار گرفته است.

فناوری بلاک‌چین ظرفیت بالقوه‌ای برای تبدیل شدن به یک سامانه موازی امن و راحت برای نقل و انتقالات مالی در نظام بانکی دارد. با استفاده از این فناوری در انجام پرداخت بین بانکی، هزینه‌ها بسیار کاهش خواهد یافت و سرعت معاملات بالا خواهد رفت. بانک‌های بزرگ در سراسر جهان با استفاده از فناوری بلاک‌چین به دنبال کاهش تعداد افراد دخیل در معاملات هستند. همچنین با این روش، کارایی عملیات میان بانک‌ها افزایش می‌یابد و مدل‌های کسب و کار جدیدی شکل می‌گیرد. بانک‌های مرکزی در سراسر دنیا در حال بررسی امکان استفاده از فناوری بلاک‌چین در سامانه‌های پرداخت خود یا استفاده از این فناوری جهت راه‌اندازی ارز دیجیتال مخصوص خود هستند.^۴

اهمیت اساسی بلاک‌چین در نظام مالی بین‌المللی در این است که معاملات را به صورت کاملاً توزیع شده انجام می‌دهد و از ذخیره سازی اطلاعات در یک پایگاه متمرکز جلوگیری می‌کند. همچنین نظارت و ایجاد محدودیت توسط شخص ثالث

1. Blockchain

2. Block

3. Chain

4. Techbullion.com/will-2018-give-us-reasons-blockchain-technology-importance/

را به کلی حذف می‌نماید. این رویه بر خلاف سامانه‌های پرداخت بین‌المللی از قبیل سوئیفت است که معاملات در آنها به صورت متمرکز و تحت نظارت کشورهای خاص صورت می‌پذیرد. لذا توسعه فناوری بلاک‌چین این انگیزه را در بین کشورهای تحت تحریم یا سایر کشورهایی که در استفاده از سامانه‌های پرداخت بین‌المللی دچار محدودیت هستند، ایجاد می‌کند که سامانه‌های پرداخت مبتنی بر فناوری بلاک‌چین را مختص خود و موازی با سامانه‌های پرداخت بین‌المللی ایجاد نمایند.

در حال حاضر تحولات در زمینه ایجاد پیام‌رسان‌های مالی موازی سوئیفت مبتنی بر بلاک‌چین نیز به طور چشم‌گیر و با سرعت فزاینده پیش می‌رود. به عنوان نمونه می‌توان به پیام‌رسان مالی ریپل^۱ اشاره کرد. این پیام‌رسان در حال حاضر با روند روبه‌رشدی در حال پذیرش و استفاده توسط بانک‌ها و کشورهاست و پیش‌بینی‌ها بر این است که در آینده به موازی جدی برای سوئیفت تبدیل خواهد شد.

البته شکل‌گیری پیام‌رسان‌های مالی موازی سوئیفت که بر فناوری بلاک‌چین مبتنی هستند، فقط به پیام‌رسان ریپل ختم نمی‌شود و در حال حاضر بانک‌های بین‌المللی بزرگی از کشورها مختلف اقدام به راه‌اندازی و استفاده از پیام‌رسان‌های مالی موازی سوئیفت متعددی نموده‌اند.

ظهور و تقویت FATF واکنش جدید آمریکا به اقدامات کشورها

پس از افشای دسترسی بی‌حد و حصر آمریکا به سوئیفت و مشخص شدن آثار منفی همکاری با این پیام‌رسان، کشورها به تدریج مسیرهای جدیدی را باز نمودند تا رفته رفته وابستگی خود به سوئیفت را کاهش دهند. اما پیش‌بینی این مسئله که دیگر سوئیفت به عنوان تنها مرجع ثبت اطلاعات مالی نخواهد بود، باعث شد تا نهاد دیگری تحت عنوان گروه ویژه اقدام مالی یا FATF به عنوان یک سازوکار مکمل توسط آمریکا در نظام مالی جهانی ایجاد و توسعه داده شود.

جالب توجه اینجاست که FATF از سال ۲۰۰۱ تشکیل شده، اما توسعه فعالیت هایش در قالب جدید، به سال ۲۰۱۲ و همزمان با آغاز حرکت عملیاتی کشورها به سمت ایجاد پیام‌رسان‌های موازی سوئیفت بر می‌گردد. ثبت اطلاعات در FATF روشی متفاوت از سوئیفت دارد؛ کشورهای عضو این گروه موظف هستند بر اساس درخواست اعضا و طبق پروتکل‌های ارائه شده، اطلاعات مالی خود را ارائه و افشا نمایند. طبق این سازوکار، از این به بعد قرار است FATF به عنوان مکمل سوئیفت، نقش ویژه برای شناسایی شریان‌های اقتصادی کشورها داشته باشد و آمریکا از طریق آن، جریان‌های مالی کشورهای مدنظر خود را شناسایی کند. این سازوکار، با توجه به اینکه روش اجماع و مطالبه جهانی را جهت دریافت اطلاعات انتخاب کرده، اثرگذاری قابل توجهی در فشار به کشورها خواهد داشت.

وزارت خزانهداری آمریکا برای تقویت حضور خود در گروه ویژه اقدام مالی (FATF) برنامه‌ریزی ویژه‌ای کرده است. به عبارتی آمریکا از این طریق نیز به دنبال آن است که داده‌های مالی مورد نیاز برای افزایش شفافیت مالی کشورهای جهان نزد خود را افزایش دهد. در همین زمینه خوان زاراته معاون سابق مدیریت مبارزه با تروریسم و جرائم مالی در وزارت خزانهداری آمریکا در کتاب خود تحت عنوان «جنگ خزانهداری» بیان کرده است که در کنار تلاش‌های متعدد آمریکا برای دسترسی به داده‌های مالی بین‌المللی «در عین حال ما تلاش کردیم تا این مسأله را روشن کنیم که دسترسی به داده‌های حوزه نقل و انتقالات مالی بین‌المللی، یک هدف مشترک بین‌المللی است که بر اساس استانداردهای FATF و بهترین شیوه‌ها انجام می‌شود.»

در کتاب جنگ خزانهداری، در رابطه با میزان موفقیت آمریکا در استفاده از داده‌های مالی کشورها موارد متعددی آورده شده است. یکی از این موارد، استفاده آمریکا از داده‌های سوئیفت برای ردیابی یکی از اعضای گروه القاعده است که در حادثه ۱۱ سپتامبر دخیل بوده است. آمریکا همچنین موارد دیگری از ردیابی مالی افراد و نهادها

را از طریق سوئیفت انجام داده است. اما با وجود دسترسی آمریکا به داده‌های مالی سوئیفت، زاراته می‌گوید در ماه‌های بعد از حادثه ۱۱ سپتامبر، وزارت خزانه‌داری آمریکا شبکه‌هایی از حواله را مورد هدف قرار می‌دهد که برای انتقال پول به القاعده استفاده می‌شده است؛ که تا حدودی این شبکه توسط وزارت خزانه‌داری از بین برده شد. زاراته در ادامه می‌گوید: اما ما متوجه شدیم که نظام حواله به طور کلی نمی‌تواند نابود شود و از طرفی هم می‌دانستیم که می‌تواند برای اهداف مهمی مورد استفاده قرار گیرد، لذا مشخص کردیم که باید نظام حواله تنظیم شود و در قالب یک چارچوبی بتوان معاملات آن را تحت نظارت داشت.

به گفته زاراته، در نتیجه پیشنهاد ویژه ای که در سال ۲۰۰۱ در FATF تصویب شد، این بود که مقررات مربوط به رمیتنس (انتقال وجه خُرد) و سامانه‌های غیررسمی از جمله حواله تنظیم شود و نتیجه این شد که طبق یک نقشه راه، کشورها سامانه‌های حواله‌ای خود را تنظیم کنند. به عبارتی دیگر، در نظارت آمریکا بر داده‌های مالی کشورهای جهان جهت مبارزه با پولشویی و تأمین مالی تروریسم، در گام اول از داده‌های سوئیفت برای رصد نظام بانکداری بین‌المللی استفاده می‌شود. در گام دوم نیز سامانه‌های غیررسمی از قبیل حواله و پرداخت‌های خارج از نظام بانکی، از طریق گروه ویژه اقدام مالی (FATF) پیگیری و تنظیم می‌شود.

بر این اساس، عضویت ایران در FATF و اجرای درخواست‌های آن، همان مسائلی را برای اقتصاد ایران ایجاد می‌کند که سوئیفت طی سال‌های اخیر ایجاد کرده و در واقع پازل آن را تکمیل خواهد کرد. لذا ضروریست از این تجربه بزرگ درس گرفته شود و تدابیر لازم برای جلوگیری از آنچه سوئیفت بر سر اقتصاد ایران آورد، اندیشیده شود.

بخش نهم

پیشنهادها

سوئیفت مهمترین ابزار شناسایی آمریکا در جنگ اقتصادی علیه ایران است؛ لذا ضروریست فرآیند پیام‌رسانی مبادلات خارجی ایران از وابستگی به سوئیفت خارج شود تا علاوه بر از بین رفتن امکان نظارت آمریکا، شرایط برای کاهش هزینه‌ها و افزایش سرعت مبادلات خارجی ایران فراهم گردد. به عقیده دکتر کلارا پورتلا، استاد دانشگاه آمریکایی و متخصص سیاست تحریم، تحریم سوئیفت در دوره قبل تحریم‌های ایران، اثرگذاری قابل توجهی بر کاهش فروش نفت این کشور داشت؛ اما چنانچه در دوره فعلی ایران بتواند راهکارهای موازی سوئیفت را برای مبادلات خود راه اندازی نماید، بازنده اصلی قطع دسترسی ایران به سوئیفت، کشور آمریکا خواهد بود.^۱

بر این اساس، ضروری است اقدامات زیر در دستور کار قرار گیرد:

الف) راه اندازی و استفاده از پیام‌رسان مالی اختصاصی در همکاری دوجانبه و چندجانبه با سایر کشورها یا اتحادیه‌ها با بهره‌گیری از آخرین فناوری‌های روز دنیا از جمله فناوری بلاک‌چین و سایر فناوری‌های مرتبط؛ در واقع جمهوری اسلامی ایران باید در همکاری با کشورهای طرف تجاری خود، از سازوکارهای مالی دوجانبه استفاده نماید و لزومی ندارد با همه کشورهای جهان، از طریق یک پیام‌رسان، مبادله نمود.

ب) استفاده از ظرفیت پیام‌رسان ملی سپام در تبادلات داخلی و بین‌المللی و ایجاد دسترسی برای بانک‌ها و مؤسسات مالی خارجی طرف قرار داد با بانک‌های ایرانی که متقاضی استفاده از پیام‌رسان‌های مالی کشور ایران هستند. در حال حاضر بعضی

1. Albawaba.com/news/europe-and-us-diverge-iran-swift-financial-network-stuck-middle-1184096

بانک‌ها و کشورها جهت استفاده از سپام ایران، تقاضای خود را ارائه نموده اند؛ در صورتی که بانک مرکزی شرایط را برای این همکاری فراهم نماید، می‌توان از ظرفیت این سامانه نیز در پیام‌رسانی مالی بین‌المللی استفاده کرد.

ج) انعقاد قرارداد همکاری با کشورها، مجامع، اتحادیه‌ها، بانک‌ها و مؤسسات مالی منطقه‌ای و بین‌المللی که در زمینه ایجاد پیام‌رسان‌های مالی موازی سوئیفت اقدام کرده اند به منظور استفاده از ظرفیت آنها؛ به عنوان نمونه در تعامل با کشورهای چین و روسیه می‌توان از پیام‌رسان‌های این دو کشور در مبادلات استفاده نمود.

د) تأمل و احتیاط بیشتر در پیوستن به FATF در چارچوب فعلی همکاری این نهاد؛ با توجه به آنچه آمریکا از طریق این کارگروه به دنبال آن است و به نوعی تکمیل شناسایی از طریق سوئیفت را با آن دنبال می‌کند، ضروری است در پیوستن به آن احتیاط بیشتری شود و با تأمل در تعهدات و اقداماتی که بایستی ایران انجام دهد و همچنین مزایا و معایب آن برای اقتصاد کشور، از تعجیل بی‌مورد جلوگیری شود.



استقلال به معنای قهر کردن با کشورها نیست، به معنای ایجاد کردن
سدّی در مقابل نفوذ کشورها است که نتوانند منافع آن کشور را، منافع
ملّت را تحت الشّعاع منافع خودشان قرار بدهند؛ این معنی استقلال است و
این مهم‌ترین هدف برای یک کشور است.

دیدار با فرماندهان و کارکنان نیروی هوایی ارتش - ۱۹ بهمن ۱۳۹۲



تهیه شده در شبکه تحلیلگران اقتصاد مقاومتی