امنیتی‌سازی تنش سایبری جمهوری اسلامی ایران و عربستان سعودی؛ تهدیدها و الزامات راهبردی

محمد داوند*

احمد سلطانی‌نژاد**

چکیده

امنیتی‌کردن گفتمان سایبری، جمهوری اسلامی ایران را در مسیری بحرانی قرار خواهد داد که عدم اتخاذ راهبردهای مناسب در برابر آن، ابعاد احتمالی بین‌المللی مانند پرونده هسته‌ای در پی خواهد داشت. پس از وقایع سال ۲۰۱۱ در غرب آسیا و شمال آفریقا، تنش نظام‌مند ایران و عربستان به فضای مجازی سرریز شد. در کشاکش تنش سایبری دو کشور در ۱۵ آگوست ۲۰۱۲، تأسیسات سایبری شرکت آرامکو عربستان مورد حمله سایبری قرار گرفت. متخصصان آمریکایی مسبب حمله سایبری به آرامکو را ایران معرفی کردند. پس از این واقعه، گفتمان سایبری جمهوری اسلامی ایران از جانب هم‌پیمانان عربستان، به‌ویژه ایالات‌متحده در معرض امنیتی‌سازی قرار گرفت. حال این پرسش‌ها مطرح هستند که تنش سایبری ایران و عربستان چگونه به فرایند امنیتی‌کردن گفتمان سایبری جمهوری اسلامی ایران دامن می‌زند؟ و امنیتی‌کردن گفتمان سایبری ایران چه ابعاد و عناصری را در بر دارد؟ نویسندگان در پاسخ پرسش‌های پژوهش، امنیتی‌کردن و ابعاد آن را شامل سه مرحله می‌دانند: (۱) کشورهای هم‌پیمان سعودی سعی در معرفی ایران به‌عنوان متجاوز به امنیت سایبری عربستان را دارند، (۲) این کشورها با نادیده‌گرفتن حملات سایبری عربستان علیه ایران، حملات صورت گرفته به عربستان (که عاملیت ایران در اجرای آنها اثبات نشده) را به‌مثابه تهدیدی بالقوه برای بیشتر کشورهای دنیا می‌پندارند، (۳) این تهدیدپنداری کشورهای هم‌پیمان سعودی با سازوکارهایی نظیر دگرنمایی توان سایبری ایران (افراد و نهادها) تلاشی بهانه‌جویانه در مسیر اتهام به ایران در تکمیل فعالیت‌های تروریستی، هسته‌ای و حقوق بشری است. بنابراین، نویسندگان معتقدند توجه به معضل امنیتی‌کردن گفتمان سایبری باید یکی از الزامات راهبردی ایران در سال‌های آتی باشد. رویکرد تحقیق حاضر، تحلیلی و روش گردآوردی اطلاعات، اسنادی و کتابخانه‌ای است.

واژگان کلیدی

ایران، عربستان، تهدیدهای سایبری، امنیتی‌سازی، تنش

---

* دانشجوی دکترای روابط بین‌الملل دانشگاه تربیت مدرس (نویسنده مسئول)

Email: davand@modares.ac.ir

** استادیار دانشگاه تربیت مدرس

Email: soltani@modares.ac.ir

تاریخ ارسال: ۹۶/۶/۲۹ تاریخ پذیرش: ۹۶/۱۰/۱۰

فصلنامه راهبرد / سال بیست‌وهفتم / شماره ۸۶ / بهار ۱۳۹۷ / صص ۹۸-۷۱

جستارگشایی

با ظهور و گسترش صنعت ارتباطات و در امتداد آن اینترنت به‌عنوان شبکه ارتباطی و اطلاعاتی جهانی، فضای جدیدی در عرصه زندگی بشریت به وجود آمد که می‌توان با عناوینی همچون «فضای دوم» و «فضای سایبری» از آن یاد کرد. فضای جدید به دنبال پیشرفت فناوری‌هایی که تصور «تغییر جهت بین دو فضایی» را بیش‌ازپیش «نامحسوس» و «غیرطبیعی‌زدایی» می‌کند، به‌تدریج الزامات، قواعد، هنجارها، الگوهای کنشگری، تعامل، نهادها، اجتماعات، ارزش‌ها و ضدارزش‌های فضای این جهانی را در خود به شکلی شبیه‌سازانه بر می‌سازد. اما از سوی دیگر علاوه‌بر سویه مطلوب و هنجارمند که در این فضا با سرعتی غیرقابل تصور به شکلی نمادین تصور می‌شوند، سویه‌های تاریک زندگی فردی و اجتماعی انسان‌ها در جهان واقعی نیز به این فضا سرریز شده است (عاملی و حسنی، ۱۳۹۱: ۲).

ازجمله ابعاد منفی و مهلک فضای سایبری، تهدیدها و آسیب‌هایی است که از افراد و دولت‌ها علیه یکدیگر در این فضا به وجود می‌آورند، اما نکته جالب‌تر آنکه بسته به شرایط سیاسی و بین‌المللی و فنی، برخی از دولت‌ها، دستاوردها، سیاست‌ها و اقدامات سایبری برخی از کشورها را دستمایه ایجاد تهدیدهایی جدی علیه آنها در فضای واقعی می‌کنند. یکی از کشورهایی که از این حیث در آستانه تهدیدهایی راهبردی است، جمهوری اسلامی ایران به‌واسطه تنش سایبری با عربستان سعودی است.

ایران یکی از معدود کشورهایی است که پس از وقایع سال ۲۰۱۱، کمترین آسیب به آن وارد شد و در برخی از کشورها مانند عراق و یمن به‌واسطه مبارزه با تروریسم، نفوذ راهبردی کرد. گفتمان هسته‌ای جمهوری اسلامی ایران نیز به دور از ارزیابی دستاوردها و چالش‌های آن برای بازیگران نظام بین‌الملل، حل شد. در مقابل عربستان سعودی در ژئوپلیتیک جدید غرب آسیا، درگیر بحران یمن شد؛ عراق شریک پیشین راهبردی خود را از دست داد و جبهه جدید درگیری با داعش بر روی آن گشوده شد. از این‌رو جنگ سرد بین ایران و عربستان به اوج خود رسید و تحولات آن فضای مجازی را نیز تحت تأثیر قرار داد. هکرهای سعودی، وبگاه‌های دولتی و زیرساخت‌های سخت‌افزاری و نرم‌افزاری ایران را مورد حمله قرار دادند و بسیاری از تأسیسات مجازی عربستان نیز ازجمله زیرساخت‌های سایبری آرامکو مورد حمله سایبری قرار گرفت. متعاقباً عربستان، ایران را عامل حملات سایبری به آرامکو معرفی کرد.

از زمان وقوع این حادثه تاکنون برخی از کشورها ازجمله ایالات‌متحده آمریکا، سعی داشته‌اند با تهدید جلوه‌دادن ابعاد و اضلاع آن، دستاوردهای متخصصان ایرانی در فضای سایبری را امنیتی سازند. امنیتی‌سازی گفتمان سایبری جمهوری اسلامی ایران تاکنون در قالب

اصول و مبانی «جنگ سرد» در دستور کار سیاسی هم‌پیمانان راهبردی عربستان سعودی قرار گرفته است. امنیتی‌کردن گفتمان سایبری ایران در صورتی انجام می‌گیرد که امنیتی‌سازی گفتمان‌های هسته‌ای، تروریسم و حقوق بشر با توجه به مقتضیات و ملاحظات سیاسی و بین‌المللی کارایی زیادی ندارد. از سویی گفتمان سایبری جمهوری اسلامی ایران از ظرافت‌ها و ظرفیت‌های فراوانی برای امنیتی‌کردن برخوردار است که نتایج آن می‌تواند بحران‌هایی با ابعاد بین‌المللی نظیر تهدید و تحریم (همچون امنیتی‌کردن گفتمان هسته‌ای) برای جمهوری اسلامی ایران در پی داشته باشد. از طرفی، شناسایی و تحلیل همین تهدیدات، مقدمه پیشگیری از آنها خواهد بود. در همین ارتباط پس از تحلیل ابعاد امنیتی‌سازی تنش سایبری ایران و عربستان، درنهایت مهم‌ترین الزامات راهبردی برای دفع حداکثری تهدیدات مزبور ارائه خواهد شد. در این راستا، پیشینه تحقیق نشان می‌دهد که دستاوردهای مقاله حاضر از این حیث که به شکل مستقل به تحلیل پیامدهای تنش سایبری دو کشور و نیز مهم‌ترین الزامات راهبردی آن برای ایران (با رویکرد امنیتی‌سازی) می‌پردازد، دارای نوآوری است.

پیشینه تحقیق. *سیبونی* و *کرونفلد* (۲۰۱۲) در پژوهشی با عنوان «*ایران و جنگ سایبری*» معتقدند راهبرد ایران در فضای سایبری استفاده از «زور» است. ایران تسلیحات فضای مجازی را مانند «جنگ‌های چریکی» و «تروریسم» ابزار مناسبی برای آسیب‌رساندن به جبهه‌های ژئواستراتژیک دشمن (نظیر عربستان) می‌پندارد. در همین زمینه *یلان برمن* (۲۰۱۳) در مقاله‌ای با عنوان «*بازبینی تهدیدات سایبری ایران*» می‌نویسد: «مقامات ایرانی فضای مجازی را مهم‌ترین حوزه برای مقابله غرب می‌دانند، درنتیجه سرمایه‌گذاری عظیمی در این زمینه انجام داده‌اند. ایران حملاتی علیه زیرساخت‌های سایبری ایالات‌متحده و عربستان سعودی ترتیب داده است». *برونک* و *رینگاس* (۲۰۱۳) نیز در مقاله «*هک یا حمله؟ شمعون و تکامل درگیری سایبری*» می‌نویسند: «ایران به‌واسطه ویروس شمعون در آگوست ۲۰۱۲، به تأسیسات آرامکو حمله کرد. آرامکو نقشی تعیین‌کننده در بازار انرژی جهانی دارد و بزرگ‌ترین تولیدکننده نفت جهان است. شمعون در سیستم‌ها و رایانه‌های شخصی آرامکو اختلال ایجاد کرد و باعث اختلال در فرایند تولید و فروش محصولات آن شد».

لوئیس (۲۰۱۴) نیز در تحقیقی که برای *مرکز مطالعات بین‌المللی و راهبردی آمریکا* انجام داده است، می‌نویسد: «خلیج‌فارس در حال تبدیل‌شدن به یک کانون درگیری در عرصه سایبری شده است. فضای مجازی در این منطقه، همچنین مبدل یک عرصه درگیری پنهان بین آمریکا، کشورهای عضو شورای همکاری خلیج از یک‌طرف و روسیه و ایران از سوی دیگر شده است. قابلیت‌های سایبری ایران به‌منظور کنترل اختلافات داخلی و حمله به اهداف

خارجی توسط هکرها به‌مراتب بیشتر از کشورهای عربی است». *اریک کی‌شفا* (۲۰۱۴) نیز در تحقیقی با عنوان «*ظهور ایران به‌عنوان یک قدرت سایبری*» اشاره دارد که «ایران نشان داده در حملات سایبری به اهداف خود در ایالات‌متحده و عربستان سعودی، توانایی زیادی دارد. از این‌رو ایران در تلاش است تا قدرت سایبری خود را در ردیف قدرت‌های نخست سایبری جهان قرار دهد. همین موضوع (آینده قدرت سایبری ایران) سبب نگرانی ایالات‌متحده در آینده خواهد شد».

در همین باره، *کگان* و *استیانسن* (۲۰۱۵) در تحقیقی با عنوان «*تهدیدات فزاینده سایبری ایران*» بر این عقیده‌اند که امروزه ایران تبدیل به یکی از جدی‌ترین تهدیدکنندگان فضای سایبری آمریکا و هم‌پیمانان شده است. توانایی ایران در هک‌کردن زیرساخت‌های سایبری ایالات‌متحده و عربستان در چند سال اخیر به طرز شگفت‌انگیزی افزایش یافته است. پس از لغو تحریم‌های اقتصادی پرونده هسته‌ای، ایران منابع خود را جهت تقویت زیرساخت‌های سایبری توسعه داده است. همچنین *آیزنشتات* (۲۰۱۶) در مقاله «*افزایش سایه سایبری ایران*» می‌نویسد: «تهران با استفاده از سلاح سایبر مبادرت به سرکوب مخالفان داخلی و دشمنان خارجی می‌کند. پس از کشف حمله سایبری به تأسیسات هسته‌ای ایران در سال ۲۰۱۰، جمهوری اسلامی درصدد انتقام‌جویی از ایالات‌متحده و عربستان سعودی به شیوه سایبری برآمده است. این رویدادها نشان‌دهنده تقویت توان سایبری ایران است که در سال‌های آتی می‌تواند به زیرساخت‌های حیاتی ایالات‌متحده آسیب برساند». همچنین *سیلوفو* (۲۰۱۶) در نوشتاری با عنوان «*تهدیدات در حال ظهور سایبری برای آمریکا*» بر این عقیده است که ایران در سال‌های اخیر به‌شدت بر روی قابلیت‌های خود برای جنگ سایبری سرمایه‌گذاری کرده است. وی می‌گوید: «در دوره ریاست‌جمهوری *روحانی* بودجه امنیت سایبری ایران دوازده برابر افزایش پیدا کرده است؛ و پر بی‌راه نیست اگر ایران را جزء پنج قدرت برتر سایبری دنیا محسوب کنیم. محدودیت‌هایی که ایران در زمینه برجام پذیرفته است، تأثیر به سزایی بر توسعه توانایی سایبری این کشور گذاشته است».

لذا با توجه به خلأ تحقیقاتی در این زمینه، پژوهش پیش‌رو درصدد است به این پرسش پاسخ دهد که تنش سایبری ایران و عربستان، چگونه زیرساخت‌های امنیتی‌ساختن گفتمان سایبری جمهوری اسلامی ایران را مهیا کرده است؟ نگارنده بر این باور است که ایالات‌متحده آمریکا و اسرائیل، ایران را مسبب حملاتی می‌دانند که امنیت سایبری عربستان را تهدید می‌کند و با بزرگ جلوه‌دادن ابعاد این تهدیدها (عناصر امنیتی‌سازی) و نادیده‌انگاشتن حملات سایبری عربستان علیه ایران، گفتمان سایبری جمهوری اسلامی ایران امنیتی می‌کنند.

مبانی نظری. تحولات سیاسی و استراتژیک پس از جنگ سرد باعث تغییر شدید محیط امنیتی جهان شده است. بسیاری از مسائل امنیتی که اکنون ذهن سیاست‌گذاران را به خود مشغول کرده است- مانند ملت‌گرایی و منازعات قومی، گسترش سلاح‌های تخریب گسترده و ثبات سیاسی و نظامی منطقه‌ای- نسبتاً با علائق امنیت ملی همخوانی دارد، ولی توجه به چالش‌های غیرسنتی نیز افزایش داشته است. افزایش اهمیت این مسائل جدید بازاندیشی در تهدیدهای امنیتی و تجدیدنظر درباره خود مفهوم امنیت را ضروری می‌سازد (تریف و همکاران،۱۳۸۳: ۲۲۸).

امروزه فناوری‌های اطلاعاتی و ارتباطاتی نقش به سزایی در زندگی ما دارند. وابستگی به فضای دیجیتال چه در سطوح فردی و اجتماعی و چه در مقیاس دولتی و بین‌المللی در حال افزایش است. با این‌وجود، استفاده از فناوری‌های جدید همیشه آکنده از سود و فایده نیست و ممکن است پیامدهای ناگواری نیز داشته باشد. فضای مجازی[1] به علت ویژگی‌هایی چون سرعت،[2] هزینه اندک[3] و گمنامی[4] (کاربر)، بستر مساعدی را برای جرائم و حملات مجازی فراهم آورده است. این وضعیت موجب شده تا حفاظت از فضای مجازی به یکی از راهبردهای اصلی دولت‌ها (در کنار سایر مسائل راهبردی در سطح ملی و بین‌المللی) تبدیل شود (Ciolan, 2014: 120). شایان ذکر است که امنیت سایبری- و موضوعات زیرمجموعه آن مانند سایبر تروریسم، جنگ سایبری و جرم و جنایت در فضای سایبری- در سطح سیاست‌گذاری [مقامات] باقی‌مانده است و ریشه در نظریات کلان روابط بین‌الملل همچون واقع‌گرایی ندارد (Dunn, 2013: 106, a). چرا که فلسفه اصلی نظریه واقع‌گرایی و پیامدهای آن برای روابط بین‌الملل برآمده از ماهیت شر انسان (Donnelly, 2000: 9) بر سه محور مبتنی است: (۱) دولت‌ها بازیگران اصلی در سیاست جهانی هستند؛ (۲) دولت‌ها منافع ملی خود را به شیوه عقلانی تأمین می‌کنند و (۳) «قدرت» و «امنیت» اصلی‌ترین ارزش‌ها برای دولت‌ها هستند. از این حیث، جهان‌بینی تمامی نسخه‌های واقع‌گرایی اساساً بدبینانه است و آنارشی (فقدان یک حکومت مرکزی) به نظام بین‌الملل قوام می‌بخشد؛ چراکه انگیزه بقا[5] در شرایط آنارشیک منجر به «معمای امنیتی»[6] می‌شود. واقع‌گرایان در این شرایط نیازی نمی‌بینند به فراخور واقعیات عصر دیجیتال، در نظریه خود تجدیدنظر کنند. دولت هنوز بازیگر اصلی است و امنیت در بیشتر شرایط «نظامی» تعریف

1. Cyberspace
2. Fast
3. Cheap
4. Anonymous
5. Survival
6. Security Dilemma

می‌شود. آنها عمده تهدیدات دنیای ارتباطاتی را «اقتصادی» تلقی می‌کنند و تهدیدات این حوزه را در حدی نمی‌دانند که امنیت دولت‌ها را با خطر مواجه سازد (Eriksson & Giacomello, 2006: 228-230). لیبرالیسم نیز در تبیین امنیت سایبری ناتوان است.

مهم‌ترین مفروضات نظریه لیبرالیسم در روابط بین‌الملل نیز عبارتند از اینکه دولت‌ها تنها بازیگران روابط بین‌الملل نیستند و تعداد کثیری از کنشگران دولتی و غیردولتی به مناسبات سیاست بین‌الملل شکل می‌دهند. آنها معتقدند مسائل داخلی بر رفتار بین‌المللی کشورها تأثیر می‌گذارند و نهادهای بین‌المللی در تأسیس قواعد رفتار (رژیم‌های بین‌المللی) برای دولت‌ها نقش به سزایی دارند. لیبرال‌ها همچنین بر گسترش دستور کار مطالعات بین‌المللی از مطالعات مربوط به قدرت، به مطالعات اقتصاد سیاسی بین‌الملل و وابستگی متقابل تأکید دارند (Walt, 1998: 32). لیبرال‌ها با واقع‌گرایان اتفاق‌نظر دارند که دولت‌ها اصلی‌ترین بازیگران در نظام بین‌المللی هستند، اما معتقدند که دولت‌ها تنها کنشگر نیستند. درمجموع، لیبرال‌ها به دلیل نگرشی که به دستاوردهای فناوری‌های ارتباطی و اطلاعاتی (جهانی‌شدن و وابستگی متقابل) دارند، نمی‌توانند به پرداخت پیامدهای منفی یا تهدیدات فضای سایبری مبادرت ورزند (Eriksson & Giacomello, 2007: 13-15). *ریکسون* اشاره دارد مهم‌ترین نظریه‌ای که می‌تواند ابعاد و اضلاع امنیت سایبری در روابط بین‌الملل و مطالعات امنیتی را تحلیل کند، نظریه «امنیتی‌سازی» است.

۱. نظریه امنیتی‌سازی

امنیتی‌کردن یکی از اصول اصلی مکتب کپنهاگ است. در طی دو دهه اخیر، مکتب کپنهاگ در اخذ مواضع متعادل در مطالعات امنیتی، موفقیت‌های چشمگیری داشته است. این مکتب بسیاری از معضلات امنیتی نظیر درگیری‌های قومی، معضلات بهداشتی و درمانی (بیماری ایدز) و قاچاق مواد مخدر را تبیین کرده است. با توجه به اقتضائات دغدغه‌های امنیتی جدید، مکتب کپنهاگ تأکید می‌کند که صورت‌بندی مباحثات امنیتی در حال شکل بخشیدن به مراجعی از تهدیدات است که لزوماً دولت‌ها نیستند و الزاماً بخش‌های نظامی یک دولت را با خطر مواجه نمی‌کنند؛ بنابراین، این مکتب ضمن اینکه از سطح مطالعات سنتی امنیت (دولت‌محوری)[۷] فراتر می‌رود، درک درستی از امنیت و قدرت به‌واسطه منطق عرضه خود ارائه می‌دهد. در این صورت، مفهوم «امنیت» ترکیبی از ملاحظات «امنیت ملی»، (در امنیت ملی حفظ اقتدار دولت برای رفع تهدیدات دشمن بسیار اساسی است) «توانایی اخذ تصمیم» و «کارایی اتخاذ اقدامات

7. Statecentric

مبتنی بر تصمیمات صحیح» را (در برابر تهدیدات جدید) در بر خواهد داشت (Hansen & Nissenbaum, 2009: 1152).

بنابراین، از منظر نظریه امنیتی‌سازی دولت‌ها، جوامع و افراد به‌طور فزاینده‌ای به اطلاعات،[۸] سیستم‌ها و فناوری‌های مبتنی بر سایبری وابسته شده‌اند. پس طیف وسیعی از بازیگرانی که می‌توانند مورد تهدید واقع شوند، به نظریه امنیتی‌سازی اعتبار می‌دهند. همچنین تمایل به استفاده از فضای سایبری تهدیدات جدیدی را پدید آورده است که از پایان جنگ سرد، امنیت بوروکراسی‌ها را با خطر مواجه کرده است؛ و فناوری‌های ارتباطاتی از پایان دهه ۱۹۹۰ به دلیل آسیب‌پذیری رایانه‌ها، بستر مساعدی برای «امنیتی‌شدن» فراهم آورده‌اند. پس به‌منظور درک چگونگی فضای سایبری در فرایند «امنیتی‌شدن» فقط باید آن را به‌مثابه یک دستور کار سیاسی صرف، مدنظر داشته باشیم (Balzacq & others, 2016: 452-501).

محیط امنیتی معاصر به‌طور عمیقی، به سیاسی کردن یک مسئله در پیوند است. سیاست‌های امنیت صرفاً در مورد تهدیدهای از پیش تعیین‌شده نیست؛ بلکه عملی برجسته است و مسائل شخصی را به‌مثابه تهدید آشکار می‌کند. در کل، انگاره امنیتی‌کردن به‌مثابه روندهای برساختگی امنیت، توجه به پیوندهای نمادین میان امنیتی‌کردن و شکل‌های هویت‌های سیاسی جمعی را ترسیم می‌کند؛ بنابراین، امنیتی‌کردن ایجاد فضای بین‌الاذهانی و توجیه تهدیدهای وجودی با شاخص‌های کافی در جهت نتایج قابل توجیه سیاسی است (ابراهیمی، ۱۳۹۳: ۱۸-۱۶).

از نگاه نظریه امنیتی‌سازی، دو مقوله قدرت و سیاست در دنیای مجازی تلویحاً بر اهمیت انگاره‌ها و نمادها تأکید دارند. مطالعه «سیاست نمادین» (استفاده و سوءاستفاده از نمادها برای مدیریت‌کردن گفتمان‌های سیاسی و افکار عمومی) با مطالعات امنیتی عصر دیجیتال بسیار مرتبط است. یکی از کارکردهای دیگر تحلیل سازه‌انگارانه ذیل نظریه امنیتی‌سازی، تحلیل جایگاه و تأثیر زبان در محیط امنیتی دیجیتال است. به‌واسطه بهره‌برداری‌کردن واژه‌هایی نظیر «ویروس» در دنیای مجازی، جهان پیچیده فنی و انتزاعی امنیت سایبری قابل‌فهم و درواقع معنادار خواهد شد. استفاده از واژه‌هایی چون «جنگی» و «پرل هاربر الکترونیک» معنای خاصی دارد که از ذات (محیط) دیجیتالی برمی‌آید. با این‌وجود، عواقب و پیامدهای آن قابل مقایسه با پیامدهای فیزیکی جنگ متعارف نیست؛ بنابراین، تحلیل سازه‌انگارانه مکتب امنیتی‌سازی در برساختن و درک‌نمودن کنش‌های گفتاری و بلاغی کارایی زیادی دارد (Eriksson &

8. Data

(Giacomello, 2006: 235). در نگاره زیر *ریر* و *چوکری* سعی کرده‌اند تحقیقاتی کـه در ارتبـاط بـا امنیت سایبری در قالب نظریه‌های گوناگون انجام شده است را تدوین کنند.

نگاره شماره (۱)- جایگاه امنیت سایبری در نظریه‌های روابط بین‌الملل

	واقع‌گرایی	لیبرالیسم	سازه‌انگاری	بدون نظریه
جامعه مدنی جهانی			کومور (۲۰۰۱) دیبرت (۲۰۰۳) مورفی (۲۰۰۹)	
امنیت	گلدمن (۲۰۰۴) نیومیر (۲۰۱۰)		دارتنل (۲۰۰۳) در دریان (۲۰۰۳) هانسن و نیسن‌بوام (۲۰۰۹)	اریکسون و گیاکومولو
رژیم‌های اقتدارگرا		کورالس و وستاف (۲۰۰۶)		
توسعه		الدن (۲۰۰۳)		
حاکمیت	درینرز (۲۰۰۴)	نیومن (۲۰۰۸)	فارل (۲۰۰۳)	
نظریه‌های عام			هریرا (۲۰۰۳)	منجیکیان (۲۰۱۰)

(Reardon & Choucri, 2012: 5)

مبانی مفهومی. طی چند سال گذشته نگرانی‌هـای متخصصـان و سیاسـت‌گـذاران دربـاره حفاظـت از سیسـتم‌هـای اطلاعـاتی از حمـلات سـایبری افـزایش داشـته اسـت؛ و بسـیاری از کارشناسان درباره افزایش شدید حملات سـایبری (تـلاش عمـدی تبهکـارانی اسـت کـه بـرای دسترسی به فناوری‌های اطلاعاتی و ارتباطی بـا هـدف سـرقت،[9] اخـتلال،[10] آسـیب[11] یـا سـایر اقدامات خرابکارانه انجام می‌شود) در آینده هشدار داده‌انـد. بنـابراین حفاظـت از سیسـتم‌هـای ارتباطی، اطلاعاتی و محتوای آنها به‌عنوان «امنیت سایبری» شـناخته شـده اسـت، امـا امنیـت سایبری تعریف روشنی ندارد. به‌طورکلی این مفهوم به سه چیز اشـاره دارد: (۱) مجموعـه‌ای از فعالیت‌ها و اقدامات در نظر گرفته شده برای حفاظت از حملات، اختلالات یا دیگـر تهدیـدهایی که عناصر فضای مجازی به شمول رایانـه، شـبکه‌هـای رایانـه‌ای، سـخت‌افزارهـا، نـرم‌افزارهـا و اطلاعاتی که می‌توانند بـا آنهـا ارتبـاط برقـرار کننـد؛ (۲) وضـعیت و کیفیـت حفاظـت از ایـن تهدیدات؛ (۳) تلاش وافر برای اجرا و توسعه این اقدامات و کیفیت آنها (Fischer, 2014).

9. Theft
10. Disruption
11. Damage

اتحادیه ارتباطات بین‌المللی امنیت سایبری را مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی، پادمان‌های امنیتی، دستورکارها، مجموعه‌ای از روش‌های مدیریت خطر، اقدامات، آموزش، روش‌های اطمینان‌بخش، بیمه و فناوری‌هایی می‌داند که می‌تواند سازمان‌ها، افراد و دارایی آنها را در محیط سایبری در برابر تهدیدات سایبری حفاظت کند، تعریف می‌کند (Korff, 2013)؛ درنتیجه افزایش توجه افکار عمومی به تهدیدات سایبری، امنیت سایبری به یکی از مهم‌ترین مباحث در عصر دیجیتال تبدیل شده است. از زمان حملات سایبری در استونی (۲۰۰۷) تا نمایش خرابکاری‌های صنعتی ویروس استاکس‌نت[۱۲] در سال ۲۰۱۰ و موارد جاسوسی متعددی که به‌واسطه اسنودن در ۲۰۱۳ انجام گرفت؛ جنایات و تهدیدهای سایبری در حال تبدیل‌شدن به یک معضل پیچیده، پرتکرار، سازمان‌یافته و مهلک برای امنیت ملی کشورها ازجمله اتحادیه اروپا شده‌اند (Ciolan, 2014 & Cavelty, 2013, b).

به‌طورکلی مؤسسه پژوهشی *رند* درباره تهدیدات سایبری می‌نویسد: «تهدیدهای سایبری که به‌واسطه تهدیدکنندگان اتفاق می‌افتند، می‌توانند مانند تهدیدهای دنیای واقعی شامل جرم و جنایت، جمع‌آوری اطلاعات و جاسوسی، فعالیت‌های ایدئولوژیک و جنگ شوند. این تهدیدها طیف وسیعی از منابع از گروه‌های تروریستی تا گروه‌های وابسته به دولت‌های متخاصم را شامل می‌شوند» (Gribbon, 2013: 5). در نگاره زیر، *تیک* انواع تهدیدهای سایبری، انگیزه، هدف و روش آنها را مشخص ساخته است.

نگاره شماره (۲)- گونه‌شناسی تهدیدهای سایبری از حیث انگیزه، هدف و روش

	انگیزه	هدف	روش
ترور سایبری	تغییرات سیاسی	قربانیان بی‌گناه	خشونت یا اختلال به‌واسطه رایانه
هکتیویسم	تغییرات سیاسی	سیاست‌گذاران	حمله [سایبری]
کرک‌کردن	دشمنی شخصی	افراد، شرکت‌ها و دولت‌ها	حمله
جرائم سایبری	منافع اقتصادی	افراد و شرکت‌ها	باج‌خواهی، حمله، سرقت آی‌دی
جاسوسی سایبری	منافع اقتصادی	افراد، شرکت‌ها و دولت‌ها	حمله
جنگ اطلاعاتی دولت‌ها	منافع اقتصادی و نظامی	زیرساخت‌ها و دارایی‌های نظامی	حمله و حملات فیزیکی

(Tikk, 2011: 58)

12. Stuxnet

فتوحات سرزمینی در آینده ممکن است شامل گفتمان فشار،[13] پروپاگاندا و خرابکاری‌های سایبری برای وادارکردن دولت‌ها جهت تحقق خواسته‌های ما باشند. آینده تسلیحات غیرخشونت‌آمیز به ارمغان خواهد آورد. تسلیحاتی پیچیده همراه با پروپاگاندا که مرزها را در یک‌هزارم ثانیه درمی‌نوردد؛ بنابراین برخلاف کسانی نظیر *گریگوری راتری*[14] که سعی دارند بر اساس سناریوهای تاریخی با استفاده از دیدگاه سنتی، شباهت‌های وقایع ۱۱ سپتامبر و پرل هاربر را در فضای مجازی پیاده کنند؛ *شمیت* بر اساس نظریه امنیتی‌سازی، [مصادیق] امنیت سایبری را به سه دسته فنی، جنایی/ جاسوسی و نظامی/ دفاع غیرنظامی تقسیم می‌کند که در نگاره زیر بازیگران، تهدیدها و موضوعات آنها به نمایش گذاشته می‌شود (Schmidt, 2014).

نگاره شماره (۳)- مصادیق امنیت سایبری

	فنی	جنایی/ جاسوسی	نظامی/ دفاع غیرنظامی
بازیگران اصلی	کارشناسان رایانه و صنعت ضدویروس	مجریان قانون و جامعه امنیتی	کارشناسان امنیت ملی، تأسیسات دفاع غیرنظامی
موضوعات اصلی	شبکه‌های رایانه‌ای	بخش خصوصی (شبکه‌های تجاری) و اطلاعات طبقه‌بندی‌شده (شبکه‌های حکومتی)	نیروهای مسلح وابسته به مسائل رایانه‌ای و زیرساخت‌های اطلاعاتی اصلی
تهدیدهای اصلی	بدافزارها، اختلال‌های شبکه‌ای و هکرها	تهدیدهای پیشرفته مداوم، مجرمان سایبری و مزدوران دولتی	حملات هولناک به زیرساخت‌ها و حملات سایری دولت‌ها و تروریست‌ها

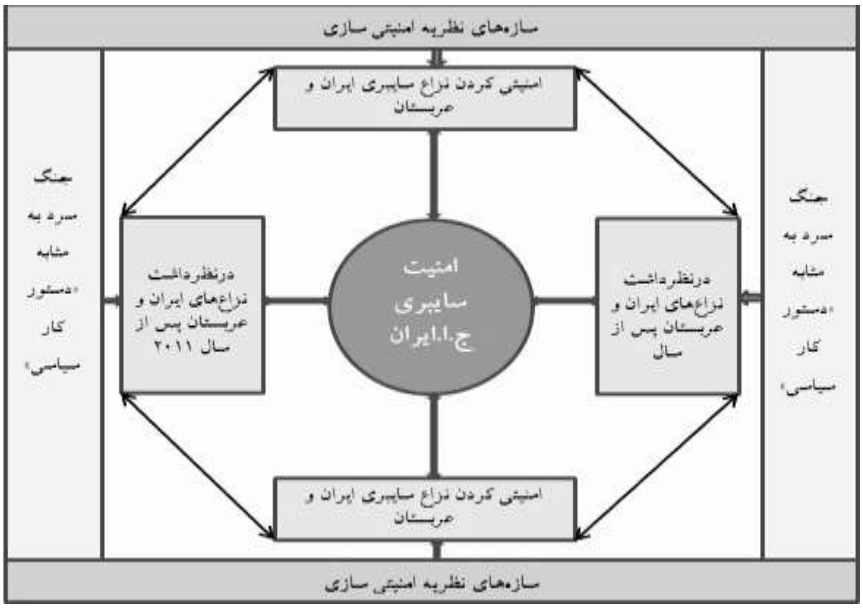
(Schmidt, 2014: 35)

روش‌شناسی. روش اصلی تحقیق حاضر، قیاسی و رویکرد آن تحلیلی است. نوع این پژوهش، کیفی، نظری و کاربردی است. شیوه گردآوری اطلاعات، کتابخانه‌ای و اسنادی و ابزارهای گردآوری داده‌ها، فیش‌برداری است. روش تجزیه‌وتحلیل داده‌ها نیز کیفی است؛ توضیح آنکه تحلیل داده‌ها بر اساس نظریه امنیتی‌سازی خواهد بود؛ یعنی در تحلیل تهدیدات عربستان سعودی علیه امنیت سایبری ایران، نویسنده درگیری عربستان سعودی و ایران را به‌مثابه یک «دستور کار سیاسی» در فضای مجازی کاربردی خواهد نمود. بهترین مجرا به‌منظور تحقق «سیاسی» یا «امنیتی‌کردن» نزاع مجازی جمهوری اسلامی ایران و عربستان

13. Discourse Pressure
14. Gregory Rattray

سعودی، «جنگ سرد» ارزیابی شد. بعد از امنیتی‌سازی تنش سایبری دو کشور، مجدداً از مبانی نظری و مفهومی نظریه «امنیتی‌سازی» جهت تحقق هدف اصلی پژوهش حاضر (بازنمایی تهدیدات سایبری امنیتی شده عربستان علیه ایران) بهره گرفته خواهد شد.

شکل (۱)- نمودار تحلیل نظری و روشی امنیتی‌سازی تنش سایبری ایران و عربستان



پس از تحقق این امر، نویسنده به تجزیه‌وتحلیل داده‌ها خواهد پرداخت. با توجه به رویکرد تحلیلی، داده‌ها با مبانی نظری و مفهومی نوشتار حاضر مطابقت داده می‌شوند. درنهایت با شناختی که از تهدیدهای امنیتی حاصل می‌شود، پردازش راهبردهایی جهت کاهش تهدیدات سایبری عربستان علیه امنیت سایبری جمهوری اسلامی ایران، در چارچوب کیفی، نظری و کاربردی بودن نوع مقاله، ارائه خواهد شد.

۲. جنگ سرد به‌مثابه یک دستور کار سیاسی در تحلیل نزاع سایبری عربستان و ایران

همان‌گونه که در مبانی نظری پژوهش گفته شد، نظریه امنیتی‌سازی در تحلیل تهدیدهای فضای مجازی و درگیری‌های سایبری بین‌المللی، دولت را به‌واسطه متغیر «دستور کار سیاسی» به حاشیه نمی‌راند. به‌عبارت‌دیگر، امنیتی‌سازی، با سیاسی جلوه‌دادن مسائل فضای مجازی آنها را به خط اصلی نزاع‌های امنیتی انتقال می‌دهد. با توجه به این مهم و کنکاش در پیشینه تنش بین ایران و عربستان، «جنگ سرد» مناسب‌ترین چارچوبی است که می‌توان از آن به‌عنوان

دستور کاری سیاسی در درگیری مجازی ایران و عربستان سعودی بهره‌برداری کرد. چرا که این دو کشور تا به حال درگیری نظامی با یکدیگر نداشته‌اند و در عوض رقابت خود را برای حفظ هژمونی و نفوذ در منطقه ادامه داده‌اند. *گرومت* روابط ایران و عربستان در مقاطع زمانی ۲۰۰۳-۱۹۷۹، ۲۰۱۱-۲۰۰۳ و ۲۰۱۱ به بعد را مدنظر قرار داده است. بر اساس آنچه از مفهوم جنگ سرد برمی‌آید در برهه‌های زمانی مذکور هفت عنصر مهم وجود دارد که نشانگر جنگ سرد بین ایران و عربستان در خاورمیانه است؛ (۱) اختلاف در ایدئولوژی سیاسی و مذهبی؛ (۲) ناکارامدی دیپلماسی؛ (۳) ایجاد اتحادهای متفاوت در سطوح منطقه‌ای و بین‌المللی؛ (۴) اختلاف در مباحث اقتصادی در منطقه خاورمیانه و جهان؛ (۵) رقابت تسلیحاتی بین دو کشور؛ (۶) شرکت در جنگ‌های نیابتی و (۷) شرکت مستقیم ایران و عربستان در جنگ‌های خاورمیانه مانند جنگ در عراق و سوریه (Grumet, 2015).

بعد از سقوط صدام در سال ۲۰۰۳، تغییراتی راهبردی در مناسبات و توازن قدرت در خاورمیانه به وجود آمد. یکی از نتایج این تحول، جبهه‌بندی‌های جدید در سطح منطقه و اتحاد جدید با قدرت‌های فرامنطقه‌ای بود. عربستان سعودی و ایران نیز به‌عنوان دو قدرت منطقه‌ای از این قاعده مستثنا نبودند؛ چرا که عربستان و ایران خواستار این هستند که پایه‌های رهبری خود در جهان اسلام را تقویت کنند. از همین‌رو تهران، ریاض را نماینده و مجری راهبردهای ایالات‌متحده آمریکا در خلیج‌فارس و منطقه می‌داند و ریاض، نگران نفوذ بیش‌ازحد تهران در منطقه پس از سقوط صدام است (Frederic & others, 2009).

به اعتقاد *گاس*، اوج جنگ سرد بین ایران و عربستان از زمانی است که «بهار عربی»[15] آغاز شد. ایران تنها برنده جنگ سرد در خاورمیانه بود و پس از سقوط نظام‌های سکولار در تونس و مصر مترصد پیروزی‌های بیشتر بود. جمهوری اسلامی ایران تحولات مزبور را ملهم و متأثر از انقلاب اسلامی ۱۹۷۹ و نه جنبش‌های عربی می‌دانست (Gause, 2015: 1-12). این شرایط خوشایند عربستان سعودی نبود. لذا عربستان سعودی پس از تحولات کشورهای عربی در نقش یک قدرت حافظ وضع موجود، بعضی‌اوقات به‌عنوان یک نیروی انقلابی سعی در سرنگونی رژیم‌های عربی ازجمله نظام بشار اسد دارد؛ اما ایران به دلایل مختلف از ایفای نقش عربستان ازجمله در سوریه جلوگیری می‌کند و سعی دارد نظام امنیتی خود را در سراسر خلیج‌فارس بگستراند. همچنین برنامه هسته‌ای این کشور تهدیدی جدی برای عربستان سعودی قلمداد می‌شود (Berti & Guzansky, 2014: 25-34).

15. Arab Spring

از همین‌روست که *گیل* معتقد است جنگ سایبری ایران و عربستان جنبه‌ای از رقابت هژمونیک این دو کشور در منطقه خاورمیانه (غرب آسیا) است. حملات سایبری که این دو کشور علیه یکدیگر انجام می‌دهند، نشئت‌گرفته از «جنگ سردی» است که بین دو کشور در جریان است. در جریان حملات هوایی عربستان سعودی به یمن در مارس ۲۰۱۵، نزاع سایبری ایران و عربستان سعودی تشدید شد. برخی از وبگاه‌های مجازی و شبکه‌های اجتماعی دو کشور در اواسط ماه آوریل هک شدند؛ و هکرهای طرفدار عربستان سعودی در ۳۱ مارس ۲۰۱۵، طی اقدامی غیرمنتظره وبگاه خبرگزاری فارس را هک کردند (Gili, 2015).

اما تهدیدهای عربستان علیه امنیت سایبری ایران همچنان ادامه پیدا کرد و در ۲۵ می ۲۰۱۶، *سردار کمال هادیان‌فر*، رئیس پلیس فتای ایران اعلام کرد: «روز گذشته هکرها طی یک حمله سایبری از سوی سه کشور که از عربستان سازمان‌دهی می‌شدند، وبگاه مرکز آمار ایران را هک کردند. وی همچنین هرگونه ارتباط هکرها با گروه تروریستی داعش را رد نمود و اذعان داشت این هکرها درگذشته نیز مبادرت به چنین اعمالی کرده بودند که پلیس فتا آنها را شناسایی کرده است». البته هادیان‌فر افزود: «دولت عربستان پشت این ماجرا نیست» (Fars News Agency, 2016). هرچند که غلامرضا جلالی، رئیس سازمان پدافند غیرعامل معتقد است پشت همه این حملات سایبری عربستان سعودی قرار دارد. جلالی با اشاره به هزینه ۶۰ میلیارد دلاری عربستان سعودی برای خرید توئیتر اختصاصی و صرف ۱۰ میلیارد دلار برای آماده‌سازی خود در پدافند سایبری، بر این باور است که عربستان خود را برای جنگ سایبری آماده می‌کند. از این‌روست که باید حملات سایبری عربستان سعودی به مراکز حساس و دولتی جمهوری اسلامی ایران ازجمله وبگاه مجازی وزارت دفاع در هفتمین روز از ماه می ۲۰۱۵ را جدی گرفت (خبرگزاری مشرق،۱۳۹۵/۰۳/۱۰).

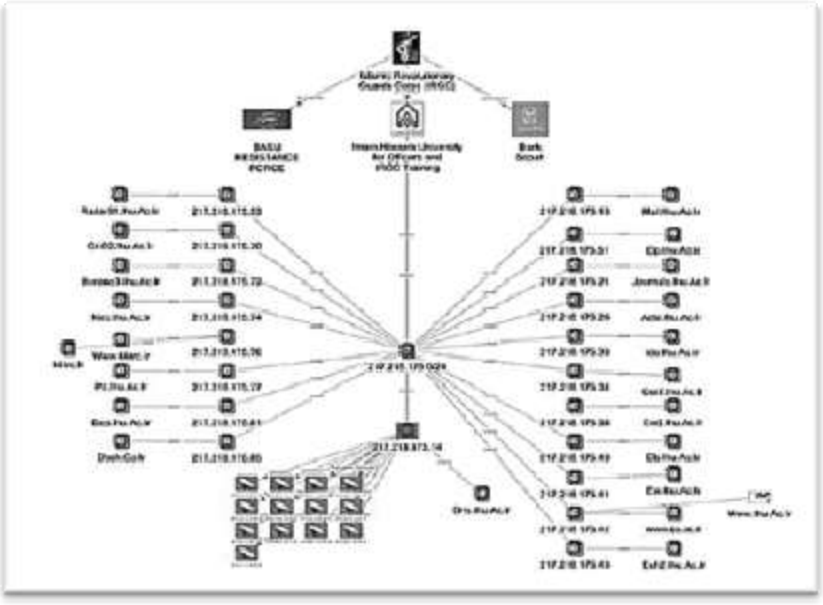
از طرفی، عربستان سعودی[(۱)] جدی‌ترین تهدید علیه امنیت سایبری خود در سال‌های اخیر را حمله سایبری ۱۵ آگوست سال ۲۰۱۲، به تأسیسات آرامکو می‌داند که در جریان آن سی‌هزار رایانه شرکت آرامکو آسیب دیدند. با توجه به اظهارات مدیران شرکت آرامکو و وزارت کشور عربستان این حمله برای ضربه‌زدن به اقتصاد عربستان با هدف تعطیل‌کردن فرایند صادرات و واردات نفت و گاز طراحی شده بود. در ماه می ۲۰۱۴، ژنرال *کیت الکساندر*[۱۶] مدیر سابق آژانس امنیت ملی آمریکا در اهمیت حمله سایبری به تأسیسات آرامکو اظهار داشت که آن «یک بیدارباش[۱۷] برای همه بود» (Oxford Business Group, 2017). خبرگزاری نیوعرب در

16. Keith Alexander
17. Wake-up

سوم دسامبر ۲۰۱۶ می‌نویسد: «بنا بـه گفتـه صـاحب‌نظـران و متخصصـان آمریکـایی حمـلات فلج‌کننده به زیرساخت‌های رایانه‌ای عربستان می‌تواند کـار هکرهـای وابسـته بـه دولـت ایـران باشد» (Traboulsi, 2016).

کگان و *استیانسن* از این فراتر رفته و ایران را بزرگ‌ترین و مهم‌ترین تهدیـد سـایبری علیـه ایالات‌متحده و متحدانش می‌دانند. به گفته آنها اندازه و قابلیت هکرهای ایرانـی در طـول چنـد سال گذشته به میزان قابل‌توجهی افزایش یافته اسـت و ایـن کشـور مـی‌توانـد در شـبکه‌هـای محافظت‌شده ایالات‌متحده و عربسـتان سـعودی نفـوذ کنـد و داده‌هـای حسـاس و محرمانـه را ضبط[۱۸] و نابود نماید؛ اما تهدیدات سایبری ایران غیرقابل مدیریت نیست، اما به‌سرعت در حـال افزایش است. تصویر زیر حملات سایبری و سیستم‌های فناوری اطلاعات دانشگاه امام‌حسین(ع) را نشان می‌دهد (Kagan & Stiansen, 2015: 2-9).

شکل (۲)- نمودار امنیتی‌سازی فعالیت‌های سایبری دانشگاه امام‌حسین(ع)



۳. امنیتی‌کردن راهبردهای ایـران در فضـای سـایبری در رویـارویی بـا عربستان سعودی

نویسنده معتقد است که در درگیری سایبری ایران و عربسـتان سـعودی اگرچـه هـر دو طـرف متحمل زیان‌های تکنیکی و فنی شده‌اند، اما همین زیان فنی عربستان، دستمایه دسـتور کـاری

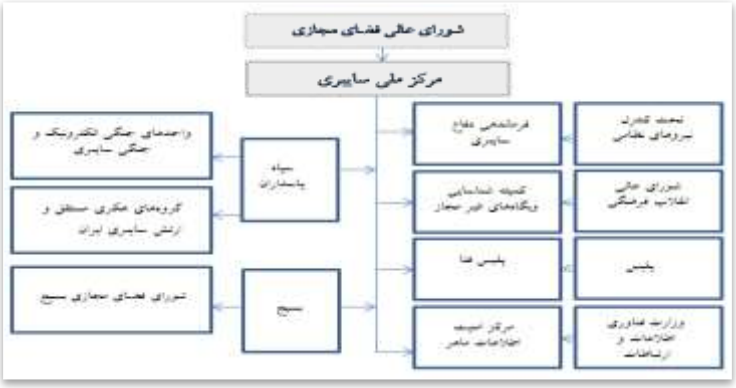
18. Seized

سیاسی قرار گرفته است که راهبردهای صلح‌آمیز جمهوری اسلامی ایران در فضای مجازی را «امنیتی» کرده است. به همین مناسبت در ادامه پژوهش ابعاد و اضلاع این موضوع تحلیل خواهد شد.

۳-۱. دگرنمایی نهادهای دفاعی و دانشگاهی ایران به‌مثابه نهادهایی تهاجمی سایبری

سیبونی و *کرونفلد* در مقاله‌ای با عنوان «ایران و جنگ‌افزارهای فضای سایبری» از توانایی‌های ایران در توسعه جنگ‌افزارهای سایبری ابراز نگرانی می‌کنند و همین موضوع را علت حمله سایبری ایران به شرکت آرامکو قلمداد می‌کنند. به اعتقاد آنها یکی از نهادهایی که توانایی تهاجمی ایران را در فضای مجازی افزایش داده است، سپاه پاسداران انقلاب اسلامی است. متخصصان غربی بر این باورند که سپاه پاسداران در زمره بهترین نهادهایی است که توانایی زیادی در زمینه جنگ سایبری در سراسر دنیا را دارد. در پژوهشی که در سال ۲۰۰۸ توسط «مؤسسه پژوهشی دفاعی تک»[19] انجام گرفت، تخمین زده شد که در [توسعه] برنامه جنگ سایبری سپاه پاسداران، حدود ۲۷۰۰ متخصص به کار گرفته شده‌اند که بودجه آن حدود ۷۶ میلیون دلار بوده است. به‌علاوه یکی از توانایی‌های سپاه پاسداران، ایجاد یک سیستم الکترونیکی جنگی است که قادر است رادارها و ارتباطات (دشمن) را قطع کند. یکی دیگر از کارکردهای سپاه پاسداران در فضای سایبری، ارتباط این نهاد با هکرهای ایرانی فعالی است که علیه دشمنان داخلی و خارجی فعالیت می‌کنند. یکی از این گروه‌های هکر، گروه «ارتش سایبری»[20] است. در شکل زیر سعی شده است تا سلسله‌مراتب نهادهای فعال در حوزه فضای مجازی در ایران به تصویر کشیده شود (Siboni & Kronenfeld, 2012, b).

شکل (۳)- سلسله‌مراتب نهادهای فعال در حوزه فضای مجازی در ایران



19. Research Institute Defense Tech
20. Cyber Army

پروپاگاندا تنها مربوط به نهادهای نظامی نیست و مراکز دانشگاهی و تحقیقاتی ازجمله دانشگاه صنعتی شریف را دربر می‌گیرد. در این رابطه کگان و استیانسن معتقدند دانشگاه صنعتی شریف یکی از مراکز دانشگاهی ایران است که امنیت سایبری بین‌الملل را تهدید می‌کند. این دانشگاه به علت پیشبرد برنامه هسته‌ای ایران، مورد تحریم‌های بین‌المللی واقع شده است. وزارت خزانه‌داری آمریکا به‌طور مستقیم برنامه‌های رایانه‌ای دانشگاه شریف را در سال ۲۰۱۲، برای تخلفات حقوق بشری مورد هدف قرار داد. خزانه‌داری ایالات‌متحده، *رسول جلیلی* رئیس دفتر همکاری‌های علمی بین‌المللی و مدیر گروه فناوری اطلاعات دانشگاه شریف و یکی از اعضای مؤسس شورای عالی فضای مجازی ایران را تحریم کرد. جلیلی به علت «تلاش برای به دست آوردن مرتبط با نظارت بر ترافیک پیام‌های کوتاه تلفن همراه از خارج»، «کمک‌های فعال به حکومت ایران جهت انجام سانسور» و «مسدودکردن وبگاه‌هایی که به انتقاد از دولت ایران می‌پرداختند» مورد تحریم واقع شد (Kagan & Stiansen, 2015: 31).

۳-۲. دگرنمایی نقش قابلیت‌های سایبری ایران در توسعه و تکمیل تهدیدات هسته‌ای

برمن می‌نویسد: «در اکتبر سال ۲۰۱۲، وزیر دفاع *لئون پانتا* آشکارا هشدار داد که ایالات‌متحده آمریکا به‌زودی با یک حادثه ناگوار جمعی با ابعادی فاجعه‌بار [یا به عبارتی دقیق‌تر] با یک پرل‌هاربر سایبری مواجه خواهد شد. در این ارتباط هیچ سناریویی فوری‌تر و به‌طور بالقوه خطرناک‌تر از بحران هسته‌ای ایران نیست. باوجود گستره عظیم فشارهای اقتصادی غرب در طول سالیان متمادی علیه ایران، نظام ایران هنوز هیچ نشانه‌ای از کاهش قابلیت‌های اتمی خود نشان نداده است. در مقابل، مقامات ایرانی با اخذ مواضع مخالف در این ارتباط، نیاز به اقتصاد مقاومتی[21] برای عبور از بحران هسته‌ای را ضروری دانسته‌اند (Berman, 2013).

سیبونی و کرونفلد معتقدند تمرکز فعالیت‌های سایبری ایران علیه عربستان سعودی و دیگران ازجمله ایالات‌متحده و اسرائیل نیاز به ترتیبات دفاعی شایسته دارد. در پرتو تحولات سایبری ایران، دولت‌های مزبور باید فضای حاکم بر فعالیت‌های سایبری جمهوری اسلامی را در دستور کار و یکی از اصلی‌ترین اولویت‌های اطلاعاتی خود (شناسایی و خنثی‌کردن حملات سایبری ایران قبل از وقوع) قرار دهند. اهمیت این موضوع درست مانند برنامه هسته‌ای ایران، می‌تواند تهدیدی مهلک علیه امنیت بسیاری از دولت‌های غربی و دولت‌های واقع‌شده در حاشیه خلیج‌فارس باشد. از این‌رو، ضروری است همکاری‌های اطلاعاتی گسترده بین‌المللی برای جلوگیری از تهدیدات سایبری ایران انجام شود (Siboni & Kronenfeld, 2012, a).

21. Economy of Resistance

۳-۳. دگرنمایی کارکردها و قابلیت‌های سایبری ایران در جهت تکمیل تخلفات حقوق بشری

فاینشنال تایمز در مقاله‌ای با عنوان «جنگ سایبری: جبهه جدیدی که ایران باز کرده است» می‌نویسد: «هکرهای ایرانی در سال ۲۰۱۲، طی حمله‌ای به تأسیسات شرکت ملی نفت عربستان سعودی (سعودی آرامکو)، تقریباً زیرساخت ارتباطاتی و اطلاعاتی این شرکت را معدوم کرده و این شرکت را تا مرز فروپاشی پیش بردند». در ادامه مقاله با اشاره به اینکه حادثه آرامکو زنگ خطری برای دشمنان ایران بود، این پرسش را مطرح می‌کند که چگونه ایران ظرف مدت چهار سال (۲۰۱۲-۲۰۰۸) به چنین قابلیت‌هایی در زمینه سایبر دسترسی پیدا کرده است؟ و پاسخ می‌دهد که بیشتر توانایی‌های ایران در فضای مجازی، حاصل تلاش این کشور به‌منظور نظارت بر معترضان نسبت به انتخابات سال ۲۰۰۹ بود (Jones, 2016).

ایزنشتات در این ارتباط می‌نویسد: «دولت قابلیت‌های سایبری خود را افزایش داد، نظارت‌های سایبری خود را بر رسانه‌های اجتماعی مضاعف کرد و به تشدید سانسور اینترنت مبادرت ورزید و از ابتدای سال ۲۰۱۲، تلاش خود را بر روی تأسیس رایانه ملی با سیستم‌عامل «لینوکس»[۲۲] مضاعف نمود و از اوایل ۲۰۱۳ سعی در ملی‌کردن خدمات ایمیل داشته است. حکومت همچنین تلاش دارد یک اینترنت ملی بدون اتصال به شبکه جهانی وب به‌منظور تقویت امنیت سایبری خود تأسیس کند» (Eisenstadt, 2016).

۳-۴. دگرنمایی کارکردها و قابلیت‌های سایبری ایران در جهت حمایت از گروه‌های تروریستی

در این رابطه *کیلفو* می‌نویسد: «ایران یکی از کشورهایی است که سرمایه‌گذاری‌های سنگینی در زمینه جنگ سایبری انجام داده است. در ایران بازار سلاح‌های سایبری وجود دارد که دشمنان ما فقط کافی است اراده کنند تا تسلیحات مزبور در اختیار آنها قرار گیرد. دستاوردها و نرم‌افزارهای مخرب ایران می‌توانند در اختیار متحد مورد اعتمادشان یعنی حزب‌الله قرار گیرد. از طرفی عناصر سپاه پاسداران انقلاب اسلامی مترصد فرصت است تا گروه‌های هکری را جذب کند. بسیج نیز به نمایندگی از رژیم از حیث تأمین نیروی انسانی برای فعالیت‌های سایبری نقش مهمی دارد» (Cilluffo, 2013).

آیتل نیز بر این باور است که ایران سابقه‌ای طولانی در حمایت از حماس دارد. حماس دارای یک تیم سایبری کوچک است که به‌هیچ‌وجه قادر به حفاظت از خود در برابر تجهیزات

22. Linux

پیشرفته فنی و اطلاعاتی اسرائیل نیست، اما با توجه به تجربه ایران، گروه سایبری حماس نه‌تنها می‌تواند از خود محافظت کند، بلکه قادر است در آینده زیرساخت‌های مالی، انرژی و نظامی اسرائیل را تهدید نماید. بنابراین، به‌جای اینکه بپرسیم که تا چه اندازه ایران قصد هک‌کردن تأسیسات ایالات‌متحده آمریکا را دارد؟ بهتر است پرسیده شود که جمهوری اسلامی ایران تا چه حد قصد هک‌کردن تأسیسات همسایگان خود ازجمله عربستان، اسرائیل و اردن را دارد؟ هدف سیاست خارجی ایران در حال حاضر تبدیل‌شدن به قدرت فائقه در خاورمیانه است (Aitel, 2015).

در پایان این بخش، نگاره زیر برجسته‌ترین ادوار تنش سایبری بین ایران و عربستان، واکنش دو کشور نسبت به این تنش‌ها و آثار سیاسی خصومت‌های سایبری ایجادشده را نشان می‌دهد.

نگاره شماره (۴)- آثار سیاسی امنیتی‌سازی تنش‌های سایبری برجسته ایران و عربستان

نام تنش سایبری	تاریخ تنش سایبری	واکنش دولتی که مورد حمله سایبری واقع‌شده (ایران و عربستان)	آثار سیاسی تنش برای کشور مقابل
اختلال در وبگاه وزارت نفت ایران	۳ و ۲۷ اردیبهشت‌ماه ۱۳۹۱	رفع نقص فنی و راه‌اندازی شبکه	-
حمله سایبری به شرکت آرامکو	۱۵ آگوست ۲۰۱۲	متهم‌کردن دولت ایران به انجام این حمله	مجرم‌شناساندن ایران به جامعه بین‌المللی و دگرنمایی قابلیت‌های سایبری ایران در مسیر کنترل مخالفان داخلی و فعالیت‌های اتمی و غیره توسط آمریکا
هک وبگاه مرکز آمار	۴ خردادماه ۱۳۹۵	مراجع ذی‌ربط از مردم خواستند در قبال این حادثه خویشتندار باشند	-
حمله سایبری به وب‌سایت‌های وزارت نفت عربستان	۱۱ آوریل ۲۰۱۵	متهم‌کردن دولت ایران به تحریک ارتش سایبری یمن به انجام این حمله	ایران از سوی رسانه‌های بین‌المللی و کارشناسان دولتی آمریکایی مقصر شناخته شد

هک برخی از وبگاه‌های وزارت خارجه	۱۳ خرداد ۹۵	پیش‌بینی حمله سایبری به زیرساخت‌های مجازی توسط رئیس سازمان پدافند غیرعامل سه هفته قبل از وقوع حمله	-
حمله‌های متعدد سایبری به وبگاه‌های سلطنتی و خصوصی عربستان	۲۰۱۶	متهم‌کردن ایران به انجام حملات گسترده سایبری در سال ۲۰۱۶	طرح مجدد اتهام کاربست ویروس شمعون (۲) توسط ایران علیه زیرساخت‌های سایبری عربستان توسط شرکت‌های آمریکایی

(منبع: یافته‌های نویسندگان)

۴. الزامات راهبردی ایران در قبال تنش سایبری با عربستان و امنیتی‌سازی آن

بعد از قیام‌های عربی سال ۲۰۱۱، نظام سیاسی کمتر کشوری در غرب آسیا و شمال آفریقا از پیامدهای این انقلاب‌ها در امان ماند. مصر تحت حکومت نظامیان قرار گرفت و انتخابات ریاست‌جمهوری با موانع زیادی روبه‌رو شد. سوریه و عراق درگیر جنگ داخلی شدند و پدیده افراطی‌گری به‌خصوص در قالب داعش در این کشورها ظهور پیدا کرد. ترکیه ناآرامی‌های فراوانی ازجمله یک کودتای ناموفق را پشت سر گذاشت اما در این میان، نفوذ سیاسی ایران در منطقه گسترش پیدا کرد؛ چرا که حکومت صدام سقوط کرده بود و اکنون شیعیان بر عراق حکومت می‌کنند. خود عراق برای دولت‌سازی و فرار از فروپاشی دولت جدید تلاش می‌کند. درواقع، عربستان سعودی یکی از بازنده‌های پیامدهای این وقایع است. عربستان باوجود اینکه از داعش حمایت می‌کند، از این هراس دارد که افراطیون داعش به عربستان تجاوز کنند. عربستان همچنین نگران آینده نفوذ خلافت اسلامی داعش در جهان اسلام و نفوذ بیش‌ازپیش ایران در منطقه است (Hussain & Kashif, 2015).

ابعاد جنگ سرد بین ایران و عربستان تا حدی رسید که فقط به رویارویی نظامی منجر نشد. عربستان سعودی در مناقشه هسته‌ای ایران نیز بر محکومیت ایران و اعمال تحریم‌های سخت‌گیرانه علیه آن پای فشرد و با تروریست‌خواندن *شیخ نمر* رهبر شیعیان عربستان، وی را اعدام کرد. با کوشش عربستان در سیزدهمین نشست سران سازمان همکاری اسلامی بیانیه‌ای تصویب شد که طبق بند ۳۳ آن، اعضای سازمان «دخالت‌های ایران در امور داخلی کشورهای

منطقه و دیگر کشورهای عضو سازمان همکاری اسلامی ازجمله بحرین، یمن، سوریه، سومالی و ادامه حمایت از تروریسم» را محکوم کردند. از طرفی، عربستان سعودی تاکنون از مجازات دو تن از مأموران پلیس فرودگاه جده که به بهانه بازرسی از دو نوجوان زائر ایرانی آنها را از کاروان جدا کرده و سپس با توسل به‌زور سعی کردند که آنها را مورد اذیت و آزار (جنسی) قرار دهند، خودداری کرده و از پرداخت دیه بیش از ۴۶۰ شهید ایرانی در حادثه منا سال ۱۳۹۴، سر باز می‌زند. به‌علاوه، سازمان حج و زیارت ایران با انتشار بیانیه‌ای اعلام کرد حج تمتع ۱۳۹۵ به دلیل استمرار کارشکنی‌های دولت سعودی برگزار نخواهد شد.

خصوصیت متمایزکننده جنگ سرد بین ایران و عربستان پس از سال ۲۰۱۱، تنش این دو کشور در فضای مجازی است. هکتویسم یکی از تهدیدهایی است که از سوی هکرهای سایبری عربستان سعودی، کارکرد برخی از وبگاه‌های مجازی دولتی و غیردولتی ایران را مختل می‌کند. به‌طورکلی مهم‌ترین وبگاه‌های ایرانی (دولتی و غیردولتی) که از سوی هکرهای عربستانی هک شده‌اند، در نگاره زیر ذکر شده است.

نگاره شماره (۵)- مهم‌ترین وبگاه‌های ایرانی مورد حمله هکرهای سعودی

نام وبگاه مجازی	تاریخ هک وبگاه	واقعه نزدیک به حمله سایبری یا علت آن	منبع
وبگاه وزارت نفت	۳ و ۲۷ اردیبهشت‌ماه ۱۳۹۱	شیعه‌ستیزی	خبرگزاری فرارو کد خبر: ۱۱۲۹۰۲
خبرگزاری فارس	۱۱ فروردین ۱۳۹۴	بحران یمن	خبرگزاری صداوسیمای جمهوری اسلامی ایران کد خبر: ۱۷۶۵۲۳
وبگاه رسمی وزارت دفاع	۱۷ اردیبهشت ۱۳۹۴	تعرض به دو نوجوان ایرانی در فرودگاه جده	مؤسسه فرهنگی مطبوعاتی ایران کد خبر: ۱۳۳۷۰۱
وبگاه مرکز آمار	۴ خردادماه ۱۳۹۵	اعلام غیررسمی جنگ سایبری عربستان علیه ایران	خبرگزاری تابناک کد خبر: ۵۹۲۸۲۹
وبگاه وزارت خارجه	۱۳ خردادماه ۱۳۹۵	اعلان غیررسمی جنگ سایبری عربستان علیه ایران	خبرگزاری الف کد خبر: ۳۵۸۷۹۷

(منبع: یافته‌های نویسندگان)

آنچه تبعات ناخوشایندی برای جمهوری اسلامی ایران در اثر تنش سایبری با عربستان در پی دارد، امنیتی‌سازی این بحران است. پس از وقوع انقلاب اسلامی در سال ۱۹۷۹، مراکز و مجامع قدرت و اندیشه‌ورزی در جهان محافظه‌کار سکولار، الگوی حاکمیتی جمهوری اسلامی را

بدیلی پرخطر برای ایجاد و اشاعه تجدیدنظرطلبی در ساختار نظام بین‌الملل، ارزیابی کرده‌اند. برای نمونه، ناگواری انقلاب اسلامی برای سیاستمداران آمریکایی تا حدی است که آنها حکومت و دولت ایران را از ابتدای تأسیس، با عناوین و عباراتی همچون «دولت توسعه‌طلب»، «ناقض حقوق بشر»، «گسترش‌دهنده سلاح‌های کشتارجمعی»، «فعال‌ترین دولت حامی تروریسم»، «اخلال‌گر در نظم منطقه»، «عضوی از محور شرارت»، «مخل روند صلح اعراب و اسرائیل»، «دولت یاغی و سرکش از نظم موجود» و «پایگاه استبداد» توصیف کرده‌اند (سلطانی‌نژاد و همکاران، ۱۳۹۱: ۱۰۸) یا شورای روابط خارجی آمریکا به‌صراحت در سال ۲۰۱۰، اعلام می‌دارد که تعامل با ایران کارساز نبوده و ایالات‌متحده باید از تغییر رژیم ایران به‌عنوان فرصتی گران‌بها استفاده کند (موسوی‌شفائی و شاپوری، ۱۳۹۰: ۱۸۹).

از این‌روست که *فیروزآبادی* در مقدمه کتاب «*امنیتی‌شدن و سیاست خارجی جمهوری اسلامی ایران*» می‌نویسد: «ایالات‌متحده آمریکا بعد از انقلاب اسلامی تلاش داشته است تا در قالب چهار گفتمان تروریسم، هسته‌ای، حقوق بشر و صلح خاورمیانه جمهوری اسلامی ایران را امنیتی کند؛ به‌گونه‌ای که این کشور به‌طور هم‌زمان یا به‌تناوب، از یکی از این گفتمان‌ها برای امنیتی‌کردن جمهوری اسلامی ایران استفاده کرده است. با این‌حال تاکنون دو گفتمان هسته‌ای و تروریسم نقش و تأثیر بیشتری در امنیتی‌کردن جمهوری اسلامی ایران ایفا کرده‌اند؛ بنابراین، امنیتی‌کردن یکی از مهم‌ترین ابعاد و موضوعاتی بوده است که جمهوری اسلامی با آن روبروست» (قریشی، ۱۳۹۳: ۱۶).

روندها نشان می‌دهد که گفتمان سایبری در دهه آینده از توان بالقوه وافری به‌منظور امنیتی‌سازی و تهدیدهای متعاقب آن برای جمهوری اسلامی ایران برخوردار است. عواملی که روند امنیتی‌سازی گفتمان سایبری را برای ایران تسریع می‌بخشند، عبارتند از:

۱) دوفضایی‌شدن (واقعی و مجازی) زندگی بشریت و کسب منافع ملی بیشتر، توسط کشورهایی که توانایی سایبری بیشتری دارند؛
۲) قابلیت‌های صلح‌آمیز فعالیت‌های سایبری جمهوری اسلامی ایران؛
۳) برجام و حل‌شدن احتمالی یا تقریبی گفتمان هسته‌ای (بدون احتساب منافع و محدویت‌های آن برای ایران)؛
۴) عملکرد متناقض غرب در قبال تروریسم و عدم کارایی مطلوب این گفتمان برای امنیتی‌سازی در رویارویی با جمهوری اسلامی ایران؛
۵) گستره وسیع مفهومی، عملیاتی و نسبی گفتمان حقوق بشر و عدم کارایی مطلوب آن[۲] برای امنیتی‌سازی در مواجهه با جمهوری اسلامی ایران.

اما عامل تثبیت‌کننده امنیتی‌سازی گفتمان سایبر، درگیری‌های سایبری ایران (دولت و یا گروه‌های هکری مستقل) و عربستان سعودی (دولت یا گروه‌های هکری وابسته دولت) یا هر کشور دیگر به‌واسطه جذابیت‌ها و توانایی‌های فنی و تبلیغاتی این گفتمان برای امنیتی‌شدن است. درواقع کشورهای محافظه‌کار سیاست بین‌الملل، پیروزی (غیرواقعی) سایبری ایران در مواجهه با عربستان را در دستور کاری سیاسی قرار داده و تبعات به‌زعم آنها خطرناک این پیروزی را به حوزه‌های دیگر انتقال می‌دهند. این کشورها به‌منظور امنیتی‌کردن گفتمان سایبری ایران با مفروض گرفتن ویژگی‌ها و قابلیت‌های تخصصی که فضای سایبری دارد، آن را مکمل تهدیدهای هسته‌ای و تروریستی جمهوری اسلامی ایران قلمداد می‌کنند.

از این حیث دولت‌های محافظه‌کار ضمن اینکه محدودیت‌های شدیدی را برای آسیب‌زدن به توانایی‌های سایبری ایران (تحریم نهادها و افراد متخصص در حوزه فضای مجازی) برنامه‌ریزی می‌کنند، از عواید امنیتی‌کردن آن نیز بهره خواهند برد.

نگاره شماره (۶)- دلایل، بسترها، عناصر و نتایج امنیتی‌سازی تنش سایبری بین ایران و عربستان

دلایل امنیتی‌سازی	زمینه‌های امنیتی‌سازی	عناصر امنیتی‌سازی	نتایج امنیتی‌سازی
نقش تأثیرگذار فضای مجازی برای افزایش منافع ملی ایران	جنبه بین‌المللی دادن به تنش سایبری ایران و عربستان	بازنمایی کارکردها و قابلیت‌های سایبری ایران در جهت حمایت از گروه‌های تروریستی	تحریم
قابلیت‌های صلح‌آمیز فعالیت‌های سایبری ایران	بزرگ جلوه‌دادن حمله‌های سایبری گروه‌های هکری غیردولتی به تأسیسات عربستان	بازنمایی کارکردها و قابلیت‌های سایبری ایران در جهت تکمیل تخلفات حقوق بشری	تهدید
ضریب اندک احتمال امنیتی‌سازی به‌واسطه گفتمان هسته‌ای	نادیده‌انگاری حمله‌های سایبری عربستان به تأسیسات ایران	بازنمایی نقش قابلیت‌های سایبری ایران در توسعه و تکمیل تهدیدات هسته‌ای	کاهش اعتبار و مقبولیت ایران نزد افکار عمومی جهانی
ضریب اندک احتمال امنیتی‌سازی به‌واسطه گفتمان تروریسم	معرفی‌کردن دولت ایران به‌عنوان کارگردان حمله‌های سایبری به تأسیسات عربستان	بازنمایی نهادهای نظامی ایران به‌مثابه نهادهایی تهاجمی سایبری	کاهش اعتبار ایران نزد سازمان‌های بین‌المللی

ضریب اندک احتمال امنیتی‌سازی به‌واسطه گفتمان حقوق بشر	تلاش برای ایجاد تنش بیشتر با تأکید بر توان تهاجمی سایبری ایران	بازنمایی نهادهای نظامی دانشگاهی ایران به‌مثابه نهادهایی تهاجمی سایبری	ائتلاف‌سازی منطقه‌ای و بین‌المللی علیه ایران

(منبع: یافته‌های نویسندگان)

با توجه به ملاحظات بالا، عناصر امنیتی‌سازی گفتمان سایبری جمهوری اسلامی ایران به‌ویژه پس از سال ۲۰۱۱ در دستور کار کشورهای محافظه‌کار قرار گرفته است. عناصر امنیتی گفتمان سایبری نتایجی مانند تحریم، تهدید و ائتلاف‌سازی منطقه‌ای و بین‌المللی علیه ایران را در پی دارد. این امر به‌واسطه شبیه‌سازی نتایج امنیتی‌سازی گفتمان هسته‌ای با گفتمان سایبر قابل استدلال است. درواقع اگر در دهه گذشته مسائل هسته‌ای و ساخت کلاهک اتمی، دستمایه امنیتی‌سازی قرار می‌گرفت؛ در حال حاضر به‌واسطه اقتضائات زمانی، حمله سایبری با «بمب سایبری» ظرفیت فراوانی جهت امنیتی‌کردن گفتمان سایبری جمهوری اسلامی ایران دارد. لذا مهم‌ترین الزامات راهبردی که نهادهای ذی‌ربط می‌توانند با اجرایی‌کردن آنها از نتایج امنیتی‌سازی گفتمان سایبر جلوگیری کند، عبارتند از:

۱) تأکید بر اینکه دولت ایران با گروه‌های هکری سایبری هیچ‌گونه ارتباطی ندارد؛

۲) انسجام و وحدت بیشتر نهادهای نظامی فعال در حوزه سایبر، به‌ویژه در زمینه اعلام نهادها یا دولت‌هایی که به تأسیسات ایران حمله سایبری می‌کنند؛

۳) پیگیری حقوقی حمله‌های سایبری و ثبت شکایت در مجامع حقوقی بین‌المللی ذی‌ربط؛

۴) برگزاری کنفرانس‌های بین‌المللی دانشگاهی و تأکید بر اینکه جمهوری اسلامی یکی از قربانیان حمله سایبری ازجمله ویروس استاکس‌نت است؛

۵) تشکیل کمیته‌ای در وزارت خارجه جمهوری اسلامی ایران به‌منظور برنامه‌ریزی برای جلوگیری از امنیتی‌سازی گفتمان سایبری و انجام اقدامات مربوطه در خارج از کشور؛

۶) قرارگرفتن امنیتی‌کردن گفتمان سایبری جمهوری اسلامی ایران در دستور کار شورای عالی امنیت ملی برای مشخص‌نمودن سیاست‌های کلی بازدارنده در این زمینه.

فرجام

تاریخ تحولات روابط بین‌الملل نشان داده است که مقتضیات زمان، به پیچیدگی‌های مفهوم «امنیت» افزوده است. به‌ویژه اینکه امروزه کشورها نمی‌توانند در معادلات امنیتی و راهبردی خود، از نقش فضای سایبری و تأثیر آن بر امنیت غافل شوند. در ارتباط با بحث حاضر، «سایبر» باوجود فرصت‌هایی که مشخصاً برای جمهوری اسلامی ایران به وجود آورده است؛ در پاره‌ای از

عرصه‌ها، باعث خلق تهدید برای امنیت آن شده است، چرا که ایران بعد از انقلاب ۱۹۷۹، در امور راهبردی، از بدنه نظم محافظه‌کارانه حاکم بر سیاست بین‌الملل گسسته و ترتیبات امنیتی بین‌المللی را نمی‌پذیرد. از این حیث، برخی از قدرت‌های بزرگ و بازیگران ذی‌نفوذ منطقه‌ای در مقابل بانفوذ و قدرت جمهوری اسلامی، از راهبرد «امنیتی‌سازی» استفاده وافر می‌کنند.

کشورهای محافظه‌کار همواره از راهبرد امنیتی‌سازی به فراخور موضوعات و مباحث مطروحه در تاریخ تحولات سیاسی و اجتماعی جمهوری اسلامی ایران، بهره‌برداری کرده‌اند. برای مثال، فعالیت‌های صلح‌آمیز هسته‌ای جمهوری اسلامی ایران طی سالیان متمادی مورد امنیتی‌سازی قرار گرفته است. این در حالی است که پاکستان، باوجود آنکه به افزایش تسلیحات هسته‌ای خود به شکل غیرقانونی مبادرت می‌ورزد، نه‌تنها کمترین نظارت‌های بین‌المللی در مورد آن اجرا نمی‌شود، بلکه در سه دوره زمانی، ریاست شورای حکام آژانس بین‌المللی انرژی اتمی را بر عهده داشته است.

بنابراین، این شرایط خاص که از جانب نظام بین‌الملل بر جمهوری اسلامی تحمیل می‌شود، تطابق زیادی با نیازها و گفتمان‌های راهبردی کشور دارد. نتایج امنیتی‌سازی گاهی در شکل تهدید، گاهی در قالب تحریم و برخی از مواقع در کالبد ائتلاف‌سازی علیه ایران، بروز کرده است. به‌طور خاص امنیتی‌سازی گفتمان سایبری، در بستر منازعات و تنش‌های عربستان سعودی و جمهوری اسلامی ایران شکل گرفته است. درواقع، پس از تنش سایبری این دو کشور در آگوست ۲۰۱۲، گفتمان سایبری جمهوری اسلامی ایران از جانب هم‌پیمانان عربستان، به‌ویژه آمریکا در معرض امنیتی‌سازی قرار گرفته است.

ابعاد امنیتی‌سازی گفتمان سایبری جمهوری اسلامی ایران از سه مجرای اصلی صورت می‌پذیرد: (الف) کشورهای هم‌پیمان سعودی سعی در معرفی‌کردن ایران، به‌عنوان متجاوز به امنیت سایبری عربستان دارند، (ب) این کشورها با نادیده‌گرفتن حملات سایبری عربستان علیه ایران، حملات صورت گرفته به عربستان (که عاملیت ایران در اجرای آنها اثبات نشده) را به‌مثابه تهدیدی بالقوه برای بیشتر کشورهای دنیا می‌پندارند و (ج) این تهدیدپنداری با سازوکارهایی نظیر دگرنمایی توان سایبری ایران (افراد و نهادها) در مسیر تکمیل فعالیت‌های تروریستی، هسته‌ای و حقوق بشری صورت می‌پذیرد.

در این میان تهدیداتی که امنیتی‌سازی گفتمان سایبری جمهوری اسلامی ایران را از دیگر تهدیدات گفتمان‌های امنیتی‌سازی برجسته‌تر می‌نماید، ظرافت‌ها و ظرفیت‌های فضای سایبر ازلحاظ فنی و محتوایی است. در حال حاضر، مسائل اتمی با فضای مجازی درهم تنیده‌اند و رسانه‌ها و فضای مجازی، ابزار مناسبی برای نمایاندن و بازنمایی وضعیت کشورها در ارتباط با

امور داخلی و خارجی آنها هستند. لذا کشورهای محافظه‌کار در سایه کشمکش سایبری عربستان و ایران، فرصت یافته‌اند تا ضمن امنیتی‌سازی گفتمان سایبری ایران، خط ربطی بین مسائل و تحولات بالا و گفتمان سایبری ترسیم کنند.

از این‌رو، اگر تهدیدات گفتمان سایبری ایران در آینده از تهدیدات گفتمان هسته‌ای و حقوق بشری بیشتر نباشد، کمتر نیز نخواهد بود؛ بنابراین، جامعه دانشگاهی کشور در راستای پیوند علم و سیاست‌گذاری موظف به ارائه راهبرد در این حیطه حساس خواهد بود. مهم‌ترین راهبردهایی که این پژوهش با بررسی دلایل، زمینه‌ها، عناصر و نتایج امنیتی‌سازی گفتمان سایبری کارامد و مفید ارزیابی می‌کند، در سه زمینه قابل بررسی هستند. نخست آنکه مقامات مسئول و ذی‌ربط جمهوری اسلامی ایران، باید در حوزه راهبردهای سایبری وحدت نظر داشته و ارتباط با گروه‌های هکری را نفی کنند. دوم، بین مجامع علمی و دانشگاهی و دستگاه‌های اجرایی، ارتباط علمی بیشتری در زمینه آسیب‌شناسی، آینده‌پژوهی و راهبردپژوهی در این حیطه برقرار شود. سوم، سازمان‌های ذی‌ربط باید حساسیت بیشتری نسبت به این موضوع نشان داده و پیگیری‌های حقوقی و سیاسی لازم در جهت کاهش امنیتی‌سازی گفتمان سایبری را در دستور کار خود قرار دهند.

پی‌نوشت‌ها:

(۱) مدارک و شواهد نشان می‌دهند که عربستان سعودی دگرگونی‌هایی اساسی در زیرساخت‌های سایبری خود ایجاد کرده است. پادشاهی سعودی بیشترین مشترکان اینترنت باند پهن در جهان عرب را داراست. از سال ۲۰۱۰ دسترسی به اینترنت در این کشور نزدیک به ۳۰ درصد افزایش یافته است. عربستان بیش از ۵۰۰ خدمات اینترنتی از طریق تلفن همراه و سیستم‌عامل‌ها برای شهروندان فراهم می‌کند. حکومت قصد دارد تا سال ۲۰۲۰ زیرساخت‌های انرژی، آب، برق و قدرت (سایبری) کشور را با استقرار شبکه‌های هوشمند و دیجیتال پیشرفته و همچنین تجهیزات تجارت الکترونیک تقویت و مضاعف کند؛ البته این مهم انجام نمی‌پذیرد مگر آنکه فناوری‌های دیجیتالی از امنیت سایبری برخوردار باشند. در سال ۲۰۱۵ عربستان سعودی بیش از ۱۶۰ هزار حمله سایبری در یک روز را ثبت کرد. بیشترین حملات سایبری متوجه بخش‌های نفت و گاز، بانکداری و ارتباطات از راه دور بود (Frontera, 2016).

(۲) به‌عبارتی‌دیگر، مخاطبی (دولت‌ها و افکار عمومی) که با گزاره عدم رعایت حقوق بشر در ایران روبه‌روست، نخستین چالش او این خواهد بود که آیا موازین حقوق بشری در کشور خود به‌طور کامل رعایت می‌شود؟ و از آنجایی که حقوق بشر مفهومی نسبی و وابسته به مقتضیات سیاسی و اقتصادی است، جذابیت امنیتی‌سازی به معنای واقعی کلمه را ندارد.

منابع فارسی

ابراهیمی، نبی‌الله (۱۳۹۳)، «بررسی مقایسه‌ای مفهوم امنیت در مکاتب متأخر امنیتی»، ***مطالعات راهبردی***، دوره هفدهم، شماره ۶۶: ۳۰-۷.

تریف، تری و همکاران (۱۳۸۳)، ***مطالعات امنیتی نوین***، ترجمه علیرضا طیب و وحید بزرگی، تهران: پژوهشکده مطالعات راهبردی.

سلطانی‌نژاد، احمد، مصطفی زهرانی و مهدی شاپوری (۱۳۹۲)، «آمریکا و برنامه هسته‌ای ایران؛ استراتژی بر چینش و ابزارهای آن»، ***مطالعات راهبردی***، دوره شانزدهم، شماره ۵۹: ۱۴۷-۱۰۷.

عاملی، سعیدرضا و حسین حسنی (۱۳۹۱)، «دوفضایی شدن آسیب‌ها و ناهنجاری‌های فضای مجازی: مطالعه تطبیقی سیاست‌گذاری‌های بین‌المللی»، ***تحقیقات فرهنگی ایران***، دوره پنجم، شماره ۱: ۳۰-۱.

قدمت چندساله جنگ سایبری ایران و عربستان (۱۳۹۵/۰۳/۱۰)، تهران: ***خبرگزاری مشرق***، کد مطلب: ۵۸۱۴۱۶.

قریشی، سیدیوسف (۱۳۹۳)، ***امنیتی‌شدن و سیاست خارجی جمهوری اسلامی ایران***، نوشته سیدیوسف قریشی با مقدمه سیدجلال دهقانی فیروزآبادی، تهران: پژوهشکده مطالعات راهبردی.

موسوی‌شفایی، سیدمسعود و مهدی شاپوری (۱۳۹۰)، «ابعاد و پیامدهای ژئوپلیتیک پرخطر ایران»، ***مطالعات راهبردی***، دوره چهاردهم، شماره ۵۴: ۱۹۲-۱۶۳.

منابع لاتین

Aitel, Dave. (2015), ***Iran is Emerging as One of the Most Dangerous Cyber Threats to the US. US: Military and Defence***, Available at: http://www.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyber-threats-to-the-us-2015-12

Balzacq, T. Léonard, S. & Ruzicka, J. (2016), "Securitization'revisited: theory and cases", ***International Relations***, Vol.30, No.4: 494-531.

Berman, I. (2013), ***The Iranian Cyber Threat, Revisited***, Statement before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

Berti, B. & Guzansky, Y. (2014), "Saudi Arabia's Foreign Policy on Iran and the Proxy War in Syria: Toward a New Chapter?", ***Israel Journal of Foreign Affairs***, Vol.8, No.3: 25-34.

Bronk, C. & Tikk-Ringas, E. (2013), ***Hack or attack? Shamoon and the Evolution of Cyber Conflict***, Institute for Public Policy Rice University.

Cilluffo, F. J. (2013), Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure, ***Testimony before the US House of Representatives, Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies***.

Cilluffo, F. J. (2016), Emerging Cyber Threats to the United States, ***Center for Cyber & Homeland Security Before the U.S***, ***House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies***.

Ciolan, I. M. (2014), "Defining Cybersecurity As The Security Issue of The Twenty First Century, A Constructivist Approach", ***Revista de Administratie Publica si Politici Sociale***, Vol.12, No.1: 40.

Donnelly, J. (2000), ***Realism and international relations***, Cambridge University Press.

Dunn Cavelty, M. (a) (2013), "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse", ***International Studies Review***, Vol.15, No.1: 105-122.

Dunn Cavelty, M. (b) (2013), A resilient Europe for an open, safe and secure cyberspace, ***Browser Download This Paper.***

Eisenstadt, M. (2016), ***Iran's Lengthening Cyber Shadow***, Washington Institute for Near East Policy.

Eriksson, J. & Giacomello, G. (Eds). (2007), ***International relations and security in the digital age***, Routledge.

Eriksson, J. & Giacomello, G. (2006), "The information revolution, security, and international relations: (IR) relevant theory?", ***International political science review***, Vol.27, No.3: 221-244.

Fars News Agency (2016), ***Cyber Police Chief: Attacks on Iranian Gov't Website Led by Saudi Hackers***. Tehran. http://en.farsnews.com/newstext.aspx?nn=13950309001116

Fischer, E. A. (2014), Cybersecurity Issues and challenges: in brief, ***Congressional Research Service.***

Frontera (2016), "***Cybersecurity in Saudi Arabia Calls for Clear Strategies***", https://fronteranews.com/news/mena/cybersecurity-in-saudi-arabia/

Gause, F. G. (2014), "Beyond sectarianism: The new Middle East cold war", ***Brookings Doha Center Analysis Paper***, Vol.11: 1-27.

Gili. (2015), The Iranian-Saudi Conflict and Its Cyber Outlet, ***Recorded Future,*** https://www.recordedfuture.com/iranian-saudi-cyber-conflict/

Gribbon, Luke. (2013), "Cyber-security threat characterization: A rapid comparative analysis", ***Rand***, Prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm.

Grumet, T. R. (2015), ***New Middle East Cold War: Saudi Arabia and Iran's Rivalry*** (Doctoral dissertation, University of Denver).

Hansen, L. & Nissenbaum, H. (2009), "Digital disaster, cyber security, and the Copenhagen School", ***International studies quarterly***, Vol.53, No.4: 1155-1175.

Hussain, M. & Kashif, M. (2015), Arab Uprising 2011: Emergence of Extremism in Middle East and Its Regional Consequences, ***Alternatives: Turkish Journal of International Relations***, Vol.14, No.2: 29-38.

Jones, S. (2016), "Cyber warfare: Iran opens a new front", ***Financial Times***, 26.

Kagan, F. W. & Stiansen, T. (2015), ***The Growing Cyberthreat from Iran: The Initial Report of Project Pistachio Harvest***, American Enterprise Institute.

Korff, D. (2013), ***Cybersecurity Definition –a selection***, Global Cybersecurity Capacity Centre.

Oxford Business Group. (2017), ***Enhancing Saudi Arabia's cybersecurity readiness***, UK. https://www.oxfordbusinessgroup.com/analysis/front-lines-enhancing-kingdom%E2%80%99s-cybersecurity-readiness

Reardon, R. & Choucri, N. (2012), "The role of cyberspace in International Relations: a view of the literature", In ***ISA ANNUAL CONVENTION*** (Vol.1).

Schmidt, N. (2014), "Critical Comments on Current Research Agenda in Cyber Security", ***Obrana a strategie***, 29-38.

Siboni, G. & Kronenfeld, S. a (2012), "Iran's Cyber Warfare", ***Institute for National Security Studies Insight***, (375), 3.

Siboni, G. & Kronenfeld, S. b (2012), "Iran and Cyberspace Warfare", ***Military and Strategic Affairs,*** Vol.4, No.3: 86-91.

Tikk, E. (2011), ***Comprehensive legal approach to cyber security*** (***Doctoral dissertation***), Tartu: Tartu University Press.

Traboulsi, Karim. (2016), "***Is Iran behind cyber attacks on Saudi Arabia?***", https://www.alaraby.co.uk/english/indepth/2016/12/3/is-iran-behind-cyber-attacks-on-saudi-arabia

Walt, S. M. (1998), "International relations: one world, many theories", ***Foreign policy***, No.110, 29-32+34-46.

Wehrey, F. Karasik, T. W. Nader, A. Ghez and Other (2009), ***Saudi-Iranian relations since the fall of Saddam: Rivalry, cooperation, and implications for US Policy,*** Rand Corporation.

Wehrey, Frederic, W. Karasik, Theodore, Nader, Alireza and Others, (2009), ***Saudi-Iranian Relations Since the Fall of Saddam:*** Rivalry, Cooperation, and Implications for U.S. Policy, ***Rand***: National Security Research Division.