تاریخ دریافت:۹۵/۱۱/۱۰
تاریخ پذیرش نهایی:۹۶/۲/۶

فصلنامه دانش امنیتی
سال اول/شماره یکم/ بهار ۱۳۹۶

بررسی تأثیرات، چالش‌ها و فرصت‌های ناشی از فناوری‌های نوین در مدیریت امنیت ملی کشور

محمدرضا یاورزاده[۱]
علی مردانی[۲]

چکیده

بی‌شک یکی از مسائلی که در دنیای کنونی از اهمیت شایانی برخوردار است و بسیاری از مسائل نظامی، اقتصادی و سیاسی را جهت می‌دهد و بر آنها تأثیر می‌گذارد، پدیده فناوری‌های نوین است که با نفوذ در همه شئون زندگی انسان، از حالات شخصی و فردی تا تعاملات جمعی اجتماعی، اقتصادی، سیاسی و فرهنگی، در حال خلق دنیایی جدید برای انسان است. در عصر سایبر با در هم تنیده شدن گسترده زندگی و تکنولوژی‌های غیربومی تهدیدهای نوینی متوجه امنیت ملی و مدیریت این فضا شده است. از آنجا که این تکنولوژی‌ها عموماً بومی نیستند و متعلق به کشورهای متخاصم یا هم‌پیمانان آنها هستند، چالش‌هایی را متوجه امنیت ملی خواهند کرد. اما نباید از فرصت‌های این فضا غافل شد.

این مقاله در پی تبیین تأثیرات، چالش‌ها و فرصت‌های استفاده از فناوری‌های نوین در مدیریت امنیت ملی کشور است. تحقیق حاضر به شیوه توصیفی و از نوع تحلیل اسنادی است و برای جمع‌آوری اطلاعات از فرم‌های فیش استفاده شده است؛ سپس اطلاعات جمع‌آوری‌شده مورد تجزیه و تحلیل قرار گرفته است. مردم و سبک زندگی، حاکمیت و قلمرو جغرافیایی، تغییر نگرش به زندگی و تحول سبک زندگی دینی به سمت سبک زندگی غربی و در نتیجه اشراف کشورهای متخاصم بر رفتار و تعاملات فردی، و کاهش حفاظت از سرمایه‌های ملی از تأثیرات و چالش‌های فناوری‌های نوین برای امنیت ملی خواهد بود. باید با درک صحیح چالش‌های پیش رو، راهبردهایی برای تقویت و شکل‌دهی به قدرت درون‌زای سایبری و ملی اتخاذ کرد.

واژگان کلیدی

فناوری‌های نوین، امنیت ملی، مدیریت

---

۱ . دکتری آینده‌پژوهی پژوهشگاه علوم انسانی و مطالعات اجتماعی جهاد دانشگاهی
۲ . نویسنده مسئول و دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات

مقدمه

در عصر حاضر با در هم تنیده شدن گسترده زندگی و فناوری‌های غیربومی، تهدیدهای نوینی متوجه امنیت ملی شده است. فضای سایبر در حال ساخت محیطی جدید در فضای فرهنگی و هویتی است. تا قبل از عصر حاضر که به عصر سایبر معروف است، هویت انسان به نژاد، قبیله و عرصه جغرافیایی استوار بود و زیست جهان مشهود و نامشهود در مکان و زمان خاص جغرافیایی، فرهنگ را تشکیل می‌داد؛ اما با شکل‌گیری و رشد سریع فضای سایبر مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام برداشت (کریمی قهرودی و کیان‌خواه، ۱۳۹۴: ۸۳). این روند موجب شد تا بسیاری از صاحب‌نظران، فضای فناوری اطلاعات و ارتباطات را به عنوان بعد چهارم قدرت و امنیت ملی در کنار ابعاد زمینی، هوایی و دریایی قرار دهند. در واقع تحولات جدید باعث شد تا قدرت‌های بزرگ در سیاست‌گذاری راهبردی و ژئوپلیتیک خود قدرت سایبری را دخالت دهند (کرامر، استار و ونتز، ۱۳۹۴: ۱۸).

از آنجا که امروزه توسعه فناوری‌های ارتباطی و اطلاعاتی از قبیل اینترنت، ایمیل، ماهواره و تلفن همراه با سرعتی درخور توجه انجام می‌گیرد، تقریباً همه دانشمندان حوزه علوم اجتماعی و متخصصان رشته‌های مختلف اتفاق نظر دارند که بهتر شدن یا بدتر شدن جهان کاملاً به این فناوری‌ها بستگی دارد (Ericsson & Gismpiaro, 2006: 221). بنابراین استفاده از فناوری‌های نوین هم می‌تواند آثاری بر دولت‌ها، توانایی‌ها و اهداف آنها در محیط داخل و بیرون داشته باشد و هم تأثیراتی بر محیط بین‌الملل بگذارد. شایان ذکر است زمانی می‌توانیم میان فناوری و آثار سیاسی آن ارتباط برقرار کنیم که فناوری را بخشی از ساختار و امری برون‌زاد نسبت به آن در نظر بگیریم (Herrera, 2003: 575). بنابراین، علاوه بر در نظر گرفتن انقلاب فناوری اطلاعات به عنوان مرحله‌ای تاریخی که به دنبال انقلاب کشاورزی و صنعتی به وقوع پیوسته است، باید آن را به عنوان یک سیاست مفهوم‌بندی کرد و به معنادار بودن و تأثیرات سیاسی- اجتماعی آن نیز توجه داشت. باید خاطرنشان کرد در میان مکاتب روابط بین‌الملل، ساخت‌گرایان اجتماعی و رهیافت‌های جامعه‌شناسی تاریخی هر دو به این بعد معنایی فناوری توجه بسیار از خود نشان داده‌اند (Herrera, 2003: 577-579).

در واقع فناوری‌های نوین اطلاعاتی- ارتباطی نوعی محیط مجازی را در عرصه بین‌المللی شکل می‌دهند. تفاوت و برتری کیفی این فناوری‌ها نسبت به فناوری‌های صنعتی مدرن این است که این فناوری‌ها موجب سرعت و دگرگونی در ماهیت تعامل

و ارتباطات جامعه بشری و همچنین ارتباط انسان با محیط اطراف و شتاب تغییرات نهادی در عرصه بین‌المللی در ابعاد اقتصادی، سیاسی، فرهنگی و اجتماعی شده‌اند (وحیدی، ۱۳۸۶: ۵۴). به همین علت فناوری اطلاعات و ارتباطات گاه فناوری آزادی نیز نامیده می‌شوند؛ زیرا توانایی‌های مردم و سازمان‌ها را برای دستیابی به داده‌ها و برقراری ارتباط بین آنها گسترش می‌دهند و انواع جدیدی از عمل را امکان‌پذیر می‌کنند که قبلاً پر هزینه و مشکل یا ناممکن بوده‌اند (Killing & Others, 2000: 21).

کلیات

۱. بیان مسئله

شالوده و بنیاد هر کشوری براساس مجموعه‌ای از زیرساختارهای حیاتی آن کشور در بخش‌های ارتباطات، دفاع، انرژی، حمل و نقل، کشاورزی، بهداشت و امور اقتصادی است که فضای سایبر با استفاده از فناوری‌های نوین به مثابه یک سیستم عصبی آنها را به هم مرتبط می‌سازد (صادقیان، ۱۳۸۷: ۱۶۶). با خلق جهان مجازی، اکنون کشورهایی در فضای مجازی وجود دارند که هر کدام شامل چندین شهر، با شهروندانی فعال و مرتبط می‌شوند؛ با این تفاوت که اهالی این شهرها شاید هیچ وقت یکدیگر را ندیده باشند، ولی ممکن است گاه در این فضا تشکل‌های اجتماعی یا صنفی منسجمی تشکیل داده باشند (قدسی، ۱۳۹۲: ۱۵۰). استفاده از فضای سایبر که دستاورد فناوری‌های نوین اطلاعات است، گرچه برای کشورهای در حال توسعه به عنوان یک فرصت برای جبران عقب‌ماندگی‌های فناورانه نسبت به جوامع پیشرفته است، اما باید دقت کرد که همین فناوری که ساخته دست این جوامع است، اگر درست بهره‌برداری نشود و حساسیت‌های امنیتی آن در مدیریت امنیت ملی مورد توجه قرار نگیرد، خود می‌تواند به عنوان یک تهدید مهم به حساب آید (ایران، ۱۳۸۲: ۵). به دنبال این تحول، توجه به توسعه علوم و فناوری‌های حوزه دفاع، امنیت ملی و سیاست خارجی اهمیتی ویژه دارد که به استعدادها و ظرفیت‌های بی‌انتهای انسانی و زیرساخت‌های مناسب پژوهشی متکی است (ولوی، طرهانی و مجردی، ۱۳۹۱: ۲۹). حوزه امنیت ملی و روابط خارجی در امر سیاست‌گذاری و ارائه برنامه‌های راهبردی و تعیین طرح‌های محوری، نیازمند انجام مطالعات کاربردی و پژوهشی است که باید به شکل مستمر مورد توجه قرار گیرد تا مبنایی برای تصمیم‌گیری در حوزه یادشده برای مبادی ذی‌ربط باشد (رستمی

و ممقانی، ۱۳۹۰: ۵۸). قدر مسلم آن است که همگان با توسعه روزافزون فناوری اطلاعات و ابزارها و شیوه‌های آن، از فرصتی طلایی بهره‌مند شده‌اند؛ اما همگام با توسعه روزافزون فناوری اطلاعات، شیوه‌های مختلف تهاجمی نیز به سرعت گسترش یافته و توان تخصصی و درجه پیچیدگی نفوذگران و عاملان تخریب امنیت ملی سیر صعودی پیدا کرده است (حسن بیگی، ۱۳۹۰: ۳ـ ۴). باید توجه کرد که امروزه اهمیت درک چنین فضایی در ارتباط با مفهوم امنیت ملی و مدیریت آن، از مهم‌ترین ادراکات ضروری برای جوامع مختلف است و این اهمیت، تلاش‌های همه‌جانبه محققان و پژوهشگران را در بازتابش روشنایی بر ابعاد مختلف موضوع طلب می‌کند (شاه‌محمدی، ۱۳۹۰: ۴۴).

۲. اهمیت و ضرورت تحقیق

پیشرفت و به‌روز بودن در حوزه امنیت ملی و دفاع از آن، نیاز به پیش‌زمینه‌هایی دارد که یکی از آنها مدیریت و توسعه علم و فناوری در این بخش است. اهمیت حوزه امنیت ملی برای کشورها ثابت‌کننده اهمیت علم و فناوری در این زمینه‌هاست. اگر علم و فناوری در این حوزه رشد اندکی داشته باشد، طبیعی است که بخش امنیت ملی و دفاع از آن نیز توسعه‌ای اندک خواهد داشت و این مسئله خسارت‌های جبران‌ناپذیری به کشور خواهد زد (ولوی، طرهانی و مجردی، ۱۳۹۱: ۵۹). سیاست توسعه علم و فناوری متناسب با امنیت ملی باید مبنای حرکت کشور در حوزه علم و فناوری باشد. کشور در تلاش برای دستیابی به برتری، نیازمند تقویت در همه ابعاد سیاسی، اقتصادی، فرهنگی، علمی و فناورانه است و سرمایه‌گذاری در این حوزه به کشور در حفظ پیشتازی در حوزه‌های مختلف کمک خواهد کرد (نیک‌سیر، ۱۳۸۴: ۷۸). اما از آنجا که ماهیت اصلی انقلاب اسلامی در تقابل با فرهنگ، اقتصاد و سیاست برخی دولت‌های غربی و سبک زندگی آنها شکل گرفته است، فناوری‌های نوین چالش‌هایی را متوجه امنیت ملی جمهوری اسلامی کرده است (سلطانی‌نژاد و اسدی‌نژاد، ۱۳۹۲: ۸۲) و تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردارند و بازیگران آن را دولت‌ـ ملت‌هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شود و ناکارامد به حساب آید (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۶۸). بررسی تأثیرات و چالش‌های

مرتبط با مدیریت امنیت ملی با گسترش فناوری‌های نوین که با سرعت زیادی درون جامعه ما در حال نفوذ است، قدم اول در حذف آسیب‌پذیری‌های این حوزه است (عطارزاده، ۱۳۹۲: ۶).

۳. هدف تحقیق

هدف اصلی این تحقیق بررسی تأثیرات فناوری‌های نوین بر امنیت ملی و مدیریت آن و شناسایی چالش‌های نوپدید بر ارکان مدیریت امنیت ملی جمهوری اسلامی است.

۴. ابزار گردآوری داده‌ها

در این تحقیق از فرم‌های فیش‌برداری به منظور گردآوری نتایج مطالعات مرتبط استفاده است.

ادبیات تحقیق

۱. تعاریف و اصطلاحات

الف) امنیت ملی

تعاریف مندرج در فرهنگ‌های لغت درباره مفهوم کلی امنیت روی «احساس آزادی از ترس» یا «احساس ایمنی» که ناظر بر امنیت مادی و روانی است، تأکید دارند. چند بعدی بودن مفهوم امنیت ملی سبب شده است دیدگاه‌های بسیار متنوعی درباره آن وجود داشته باشد و هرکس از زاویه خود به تعریف آن بپردازد. در همین راستا، برخی از نظریه‌پردازان، امنیت ملی را معادل ارزش‌های حیاتی کشور می‌دانند، آن‌گونه که آرنولد ولفرز آن را برابر «نبود تهدید برای ارزش‌های اکتسابی می‌داند» (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۵).

بری بوزان امنیت ملی را «رهایی از تهدید و توانایی دولت و جوامع برای حفظ هویت مستقل و یکپارچگی کارکردی در مقابل نیروی تغییردهنده» تعریف می‌کند (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۶). در عین حال، یکی از کامل‌ترین تعاریف را والتر لیپمن، پژوهشگر آمریکایی، ارائه کرده است: «یک ملّت وقتی دارای امنیت است که در صورت اجتناب از جنگ بتواند ارزش‌های اساسی خود را حفظ کند و در صورت اقدام به جنگ بتواند آن را پیش برد» (نصیری، ۱۳۸۴: ۸۴).

سرکسیان و همکارانش (۲۰۰۸) امنیت ملی را «تلاش دولت‌ها برای تأمین امنیت

شهروندان، تمامیت ارضی کشور و به حداقل رساندن تهدیدهای دشمنان نسبت به ارزش‌های جامعه» تعریف کرده‌اند (Sarkisian, Williams, & Cimbala, 2008: 14).

اما می‌توان گفت اوانس و نیوهم (۱۹۹۸) کامل‌ترین تعریف را برای مفهوم امنیت ملی ارائه کرده‌اند که به شرح زیر است: «مجموعه متکثری از ارزش‌ها و اولویت‌هایی که برخی متغیر و بعضی ثابت‌اند و در زمان و مکان‌های متفاوت، در تعامل با محیط بین‌الملل و داخلی، به شکل‌های مختلف به عنوان منافع ملت بر زبان سیاستمداران جاری می‌شوند» (Evans & New Ham, 1998: 345).

ب) مدیریت

تعریفی مورد قبول و عام از مدیریت در دست نیست. صاحب‌نظران و مؤلفان مدیریت با اهداف و سوگیری‌های مختلف، تعاریف گوناگون ارائه کرده‌اند. در اینجا برخی از این تعاریف را بیان می‌کنیم:

مدیریت عبارت است از:

ـ هنر انجام دادن کار به وسیله دیگران و ایجاد محیطی مؤثر برای افرادی که در گروه‌های رسمی سازمان فعالیت می‌کنند (علاقه‌بند، ۱۳۷۴: ۱۴).

ـ هماهنگ‌سازی منابع انسانی و مادی در جهت تحقق هدف‌ها (علاقه‌بند، ۱۳۷۴: ۱۳)؛

ـ فراگرد هماهنگ‌سازی فعالیت فردی و گروهی در جهت هدف‌های گروهی (Donnelly, 1975: 15)؛

ـ فرایند به کارگیری مؤثر و کارامد منابع مادی و انسانی در برنامه‌ریزی، سازماندهی، بسیج منابع و امکانات، هدایت و کنترل که برای دستیابی به اهداف سازمانی و براساس نظام ارزشی مورد قبول انجام می‌گیرد (رضاییان، ۱۳۸۰: ۶).

ـ طراحی یا پدید آوردن محیطی که در آن مردمی که در گروه‌ها با هم کار می‌کنند، بتوانند به هدف‌های خود برسند (کونتز، اودائل و ویهریخ، ۱۳۷۰: ۲۵).

ج) فناوری‌های نوین

فناوری‌های نوین، رسانه‌ای گروهی از نوع الکترونیکی هستند که به حواس بینایی، شنوایی و لامسه متوسل شده‌اند و مخاطبین متنوع و زیادی را دربرمی‌گیرند. فعالیت عمده آنها سرگرمی و تفریح است و مخاطبین اصلی این رسانه را نوجوانان و جوانان تشکیل می‌دهند (خلیفه، ۱۳۹۱: ۱۳۸).

از نظر هایدگر، فناوری نوین، نحوه‌ای از انکشاف حقیقت برای انسان مدرن است که به موجب آن، نگاه انسان مدرن به عالم عوض می‌شود (ناجی، ۱۳۹۲: ۹۵).

تامپسون، فناوری‌های نوین را به مثابه اجرای سریع‌تر الگوریتم‌هایی که در گذشته به صورت دستی، یا به واسطه فناوری‌های دیگر اجرا می‌شدند، تعریف کرده است (بابایی و فهیمی‌فر، ۱۳۹۱: ۱۷۸).

تکنولوژی یا فناوری‌های نوین عبارت است از ماشین‌آلات و تجهیزات فیزیکی (سخت‌افزار)؛ تکنیک‌ها، شیوه‌ها و دستورالعمل‌ها (نرم‌افزار)، دانش چگونگی بهره‌گیری از این ابزارها، با شیوه‌های خاص (مغزافزار) که به منظور افزایش کارایی در جریان تبدیل نهاده‌ها به ستاده‌ها (فرایند تبدیل) به کار گرفته می‌شوند (لطف الهی حقی، ۱۳۸۹: ۸۳).

۳. رویکردهای نظری متفاوت به امنیت ملی

مقوله امنیت ملی مورد توجه رویکردهای مختلفی در روابط بین‌الملل قرار گرفته است. هر یک از این رویکردها براساس نگاه خاص خود به مسائلی همچون قدرت، منافع ملی، ساختار نظام بین‌الملل و مانند آنها به امنیت ملی پرداخته‌اند. در این بخش به مفهوم امنیت ملی از نگاه مهم‌ترین این رویکردها می‌پردازیم.

از دید واقع‌گرایان معتقد در سطح سیاست داخلی، مسئله‌ای به نام امنیت وجود ندارد و امنیت صرفاً در سطح بین‌المللی معنا می‌یابد؛ به بیان دیگر، امنیت ملی نزد آنان چیزی جزء امنیت بین‌الملل نیست و در این راستا ناامنی ویژگی بارز نظام بین‌الملل است (عبداله خانی، ۱۳۸۲: ۷۰). از نظر واقع‌گرایان، ناامنی اصلی‌ترین مسئله، قدرت مهم‌ترین ابزار، دولت مهم‌ترین بازیگر و جنگ بارزترین جلوه بروز ناامنی در عرصه بین‌المللی است (یزدان‌فام، ۱۳۸۶: ۷۳۱). بنابراین، محور تمرکز واقع‌گرایی در موضوع امنیت، نظامی است.

در نقطه مقابل، لیبرالیسم کلاسیک ضمن قبول وجود هرج و مرج در عرصه بین‌المللی، با انتقاد از سیاست قدرتمندانه واقع‌گرایی معتقد است صلح نه با موازنه قدرت و تسلیح هرچه بیشتر کشورها، بلکه از طریق گسترش حکومت‌های دموکراتیک در جهان میسر است. نئولیبرالیسم نهادگرا به عنوان یکی از گرایش‌های مهم لیبرالیسم نیز همانند واقع‌گرایی قبول دارد که عرصه بین‌المللی، عرصه بی‌نظمی است و چنین فضایی امنیت ملی و بین‌المللی را به خطر می‌اندازد، اما برای حفظ امنیت، راه‌حل متفاوتی وجود دارد. صاحب‌نظران این نظریه بر این باورند که برای ایجاد امنیت و

حفظ صلح باید رفتار دولت‌ها مهار و به آنها لگام زده شود و این کار با ایجاد سازمان‌ها و رژیم‌های بین‌المللی میسر است (یزدان‌فام، ۱۳۸۶: ۷۳۲).

از سوی دیگر، مکتب کپنهاگ نیز مخالف دیدگاهی است که هسته اصلی مطالعات امنیتی را جنگ و زور می‌داند. بوزان معتقد است در دیدگاه واقع‌گرایان، مفهوم پیچیده امنیت به مفهومی مترادف با قدرت کاهش پیدا کرده است (بوزان، ۱۳۷۸: ۸). از نظر مکتب کپنهاگ گرچه امنیت فردی گویای سطح مشخص و مهمی از تحلیل است، اما افراد نمی‌توانند به عنوان مرجع امنیت شناخته شوند؛ زیرا اصولاً تابع ساختارهای سیاسی عالی‌تر دولتی و بین‌المللی هستند. بنابراین، مکتب کپنهاگ نیز با رد فردمحوری در مرجع امنیت، تمرکز خود را بر دولت به عنوان محور امنیت قرار می‌دهد (عبداله خانی، ۱۳۸۲: ۷۷).

۴. تأثیر و تهدیدهای فناوری‌های نوین بر مدیریت امنیت ملی جمهوری اسلامی ایران

بسیاری از کارشناسان و تحلیلگران حوزه امنیت بر این باورند که پایان یافتن دوران جنگ سرد نه تنها موجب امن‌تر شدن جهان نشده است، بلکه به وجود آمدن چالش‌های امنیتی غیرنظامی جدیدی همچون تخریب محیط زیست، اقتصادی، سازمان‌های جنایی بین‌المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی‌تری نسبت به گذشته مواجه کرده است. براثر این چالش، متولیان و مدیران امنیت ملی کشورها با چالش‌های نوظهوری مواجه شده‌اند که این چالش‌ها تأثیرات زیادی بر مدیریت این فضا داشته است. تحلیلگران بر این باورند که اهمیت این مسائل «جدید» نه تنها بازاندیشی در تهدیدهای امنیتی، بلکه تجدید نظر درباره خود مفهوم امنیت و مدیریت آن را ضروری می‌سازد.

در عین حال، انتقاد وارد بر ادبیات موجود امنیت این است که اغلب این متون به فناوری‌های نوین به عنوان یکی از همین چالش‌های امنیتی جدید که در این زمینه بسیار هم پراهمیت به نظر می‌رسد، توجه اندکی کرده‌اند. آنچه در مورد این فناوری‌های نوین و تهدیدهای مرتبط با آن درخور توجه است، این است که ویروس‌ها، کرم‌ها، جرم‌ها، هکرها و حملات اینترنتی، امروزه واقعیت مسلم و روزمره هستند. حملات مخرب مهم با تأثیرات گسترده، فناوری‌های نوین را به عنوان یکی از بدترین تهدیدهای منافع ملی و یکی از بزرگ‌ترین چالش‌های پیش روی مدیران این فضا به تصویر کشیده است تا جایی که ایالات متحده آمریکا اعلام کرده است که این حملات را به عنوان جنگ تلقی و با آن برخورد فیزیکی خواهد کرد (روزنا و دیگران، ۱۳۹۰: ۱۴).

اما تأثیرات فناوری‌های نوین بر امنیت ملی و مدیریت آن را می‌توان به سه گزاره اصلی تقسیم کرد: اول، تهدید ثبات کشور؛ دوم، تغییر توازن قدرت ناشی از ظهور جهان چند مرکزی؛ سوم، به چالش کشیده شدن انحصار خشونت ناشی از ظهور حملات سایبری. این سه گزاره تحت تأثیر شاخص‌های فناوری اطلاعات نوین بر شاخص‌های امنیت ملی و مدیریت آن هستند که در ادامه هر کدام از آنها در ارتباط با امنیت ملی جمهوری اسلامی ایران بررسی خواهند شد.

۵. تهدید ثبات کشور

این تهدید خود از چند بعد قابل بررسی است:

الف) تهدید مدیریت نظام سیاسی و ایدئولوژی کشور: ایدئولوژی سیاسی یک کشور مشروعیت‌دهنده سیاست‌های حاکمان آن کشور است و در پرتو آن جامعه به انسجام و وحدت می‌رسد؛ بنابراین، هرگونه تردید در ایدئولوژی یک نظام می‌تواند موجب بی‌ثباتی شود؛ در حالی که فناوری اطلاعات نوین، به ویژه اینترنت، حفظ ایدئولوژی را بیش از پیش دشوار کرده و این عامل به نوعی آسیب‌پذیری برای دولت‌های حاکم تبدیل شده است. دلیل آن نیز فرصت‌هایی است که این فناوری‌ها در اختیار افراد گذاشته و مهارت آنها را برای زیر ذره‌بین بردن عملکرد دولت‌ها، شک کردن در مشروعیت آنها و بسیج سیاسی برای تحمیل خواسته‌ها افزایش داده است (نای، ۱۳۸۹: ۴۸).

ایران تجربه تغییر رژیم و اعتراض‌های سیاسی از طریق ابزارهای ارتباطاتی را در طول تاریخ خود دارد؛ برای مثال نقش رسانه‌های مطبوعاتی در انقلاب مشروطه و استفاده از نوار کاست‌ها یا رادیوهای امواج کوتاه در انقلاب اسلامی. بعد از انقلاب، با ورود فناوری‌های نوین به ایران در دهه ۱۳۷۰، فضای مجازی به محیطی برای فعالیت اپوزیسیون تبدیل شد. نمونه بارز آن در انتخابات سال‌های ۱۳۸۰ و ۱۳۸۸ است که فناوری‌های نوین از قبیل اینترنت و شبکه‌های اجتماعی نقش اساسی در حوزه عمومی داشتند و به بخش جدایی‌ناپذیر عرصه سیاسی ایران تبدیل شدند (Rahimi, 2003: 10). می‌توان گفت فناوری‌های نوین بعد از انتخابات سال ۱۳۸۸ چالش جدیدی برای مدیران امنیت ملی کشور ایجاد کردند که هنوز هم می‌توان ردپای این چالش را در مدیریت این مقوله مهم مشاهده کرد.

ب) تهدید هویت ملی و تمامیت سرزمینی: هویت ملی یک احساس جمعی مشترک است که موجب ایجاد همبستگی میان افراد در چارچوب سرزمینی مشخص می‌شود؛

بنابراین، خلق، تداوم و مدیریت چنین هویتی از سوی دولت حائز اهمیت بسیار است (رحمت الهی، ۱۳۸۴: ۹۲)؛ در حالی که ظهور فناوری‌های نوین، توانایی دولت‌ها را در این زمینه کاهش داده است. در ارتباط با ایران، این تهدید از دو بعد درخور بررسی است: اول آنکه ارزش‌های جهانی شدن که به عنوان ارزش مسلط در این فناوری‌ها قرار دارد، به دنبال قلع و قمع هویت ملی‌ـ اسلامی است. نظرسنجی‌ها در این زمینه به ویژه میان قشر جوان نیز دلالت بر تضعیف هویت ملی دارد. تهدید دیگر از بعد هویت‌های فروملی است. ایران به عنوان جامعه‌ای قومیتی همواره از سوی هویت‌های فروملی آسیب‌پذیر بوده است. امروزه فضای مجازی فرصت بسیاری را در اختیار آنها قرار داده است تا در جهت بسیج سیاسی هرچه بیشتر حرکت کنند مانند جامعه کردهای آمریکا که در فضای مجازی ایجادشده از طریق وب سایت خود به تسهیل دستیابی به اهداف ملت کرد کمک می‌کند (Mazarr, 2005: 20). توانمند شدن این گروه‌ها و تشدید فعالیت آنها، علاوه بر تضعیف انسجام ملی می‌تواند تمامیت سرزمینی را نیز با تهدید روبه‌رو سازد.

ج) تهدید ارزش‌های ملی: از آنجا که مهم‌ترین کارویژه ارزش‌های ملی حفظ همبستگی و مشروعیت‌دهنده به قواعد و ضوابط اجتماعی است، هرگونه تهدید معطوف آنها ممکن است بی‌ثبات‌کننده مدیریت نظام سیاسی یک کشور باشد. تهدید فرهنگ و ارزش‌های جامعه ایران باید از دو بعد مورد بررسی قرار گیرد: یکی تهدید ارزش‌ها به صورت یک برنامه از پیش تعیین‌شده و غیر خشونت‌آمیز به منظور تغییر نظام سیاسی کشور (Price, 2002: 55) که امروزه ظهور اینترنت شدت و دامنه این‌گونه فعالیت‌ها را وسیع‌تر کرده است. این تهدیدها که در قالب جنگ نرم صورت گرفته است، با تهدیدهای سابق یعنی نظامی و اقتصادی متفاوت است و در راستای دیدگاه ابزارگرایانه دولت‌های غربی به فناوری‌های نوین قرار دارد (Dumbrell, 2007). تهدید دیگر ارزش‌های ملی به صورت غیرعامدانه و تنها ناشی از ورود ناخواسته این فناوری‌ها به کشور است که جامعه بعد از انقلاب را به تدریج به فضایی چندارزشی تبدیل کرده است (تاجیک، ۱۳۸۱: ۱۶۵). همان‌گونه که آولین تافلر توضیح می‌دهد، هر یک از سه موج تغییرات قدرت یعنی کشاورزی، صنعتی و اطلاعات و ارتباطات به مقیاس وسیعی باعث محو فرهنگ‌های پیشین شده و شیوه‌های جدیدی از زندگی را جایگزین کرده است. در این میان سرعت موج سوم بیش از دو موج قبل است (تافلر، ۱۳۷۶: ۸۶). بنابراین، لزوماً تضعیف و تغییر ارزش‌های ملی را نمی‌توان ناشی از تهاجم فرهنگی غرب دانست.

د) تغییر توازن قدرت: علاوه بر تهدید ثبات کشور، تأثیر دیگر فناوری‌های نوین بر امنیت ملی کشورها، تغییر توازن قدرت است که در نتیجهٔ توانمند شدن بازیگران غیردولتی رخ می‌دهد. انقلاب اطلاعات بر توان و قدر نسبی دولت در مقابل بازیگران غیردولتی در نظام بین‌الملل تأثیر می‌گذارد که این تغییر توازن در بسیاری از موارد به یک نگرانی برای دولت‌ها تبدیل شده است (Riterz, 2007: 403). در ارتباط با امنیت ملی جمهوری اسلامی می‌توان به چهار بازیگر غیردولتی اشاره کرد که هرچند تاکنون تهدید جدی علیه حاکمیت دولت‌ها ایجاد نکرده‌اند، ولی فناوری‌های نوین با تقویت این گروه‌ها می‌توانند تهدیدهایی را برای امنیت ملی به وجود آورند.

هـ) سازمان‌های مدافع حقوق بشر: واقعیتی که در رابطه با نهادهای حقوق بشر ـ به رغم افزایش توانایی آنها در محیط بین‌الملل نباید نادیده گرفت ـ آن است که هرچند این‌گونه سازمان‌ها به صدور گزارش‌ها و بیانه‌های متعددی علیه نقض حقوق بشر در ایران پرداخته‌اند، ولی تأثیر جدی در ارتباط با امنیت ملی و مدیریت آن نداشته‌اند (صالحی امیری، انتخابی و سلطانی‌فر، ۱۳۸۷: ۳۳).

و) جنبش زنان: تلاش برای اسلامی کردن جامعه ایران بعد از انقلاب اسلامی، مباحث بسیاری ایجاد کرد. افزایش شهرنشینی، افزایش سطح سواد و دستیابی به آموزش و در عین حال وجود برخی ملاحظات در سیاست‌های دولت موجب مشارکت وسیع زنان در حوزه عمومی شد. به این ترتیب جنبش زنان شکل آشکاری بیشتری به خود گرفت تا جایی که برخی از سیاست‌های محافظه‌کارانه دولت در ارتباط با زنان به چالش کشیده شدند. به طور کلی نتیجه ظهور فضای مجازی در رابطه با قشر زنان، افزایش حضور آنها در این فضا به عنوان نوعی جبران کمبود حضور آنها در دنیای واقعی در مقابل مردان است. علاوه بر آن حضور چنین جنبش‌هایی می‌تواند تهدیدی برای ارزش‌های اسلامی جامعه محسوب شود.

ز) جنبش چپ‌ها: یکی دیگر از فعالیت‌های درخور توجه در اینترنت، فعالیت گروه‌هایی با گرایش‌های چپ است. بسیاری از سایت‌ها و وبلاگ‌ها درصدد متحد کردن این گروه‌ها برای اعتراض‌ها و بیان دیدگاه‌های خود و این نکته هستند که چطور اتحادیه‌ها و گروه‌های مختلف اهداف و اقدامات خود را هماهنگ سازند. ولی فعالیت‌ها بعد از انقلاب اسلامی به دلیل دست نیافتن به اهداف‌شان کم‌رنگ‌تر شده و به رغم حضور گسترده در وب تاکنون غیر از برخی اعتراض‌های دانشجویی یا اعتصاب‌های کارگری، تهدیدی برای متولیان امنیت جمهوری اسلامی نداشته‌اند.

ح) ایرانیان خارج از کشور: ایرانیان خارج از کشور با حجم گسترده در اینترنت حضور دارند و بخشی از آنها از فضای مجازی علیه جمهوری اسلامی ایران بهره می‌گیرند. عباس میلانی، یکی از سرپرستان پروژه دموکراسی ایران در مؤسسه هوور آمریکا، گفته است: «ما در تبعید می‌توانیم در عرصه ایران به طور جدی مشارکت داشته باشیم، به همان اندازه ایرانیان در داخل...». یکی از شواهد آن نیز وجود وبلاگ‌های آنهاست. بررسی که دو محقق خارجی[1] در زمینه وبلاگ‌های فارسی انجام داده‌اند، نشان می‌دهد از میان چهار گروه محتوای وبلاگ (سکولار/اصلاح‌طلب، شعر و ادبیات، مذهبی/محافظه‌کار و گروه چهارم آمیزه‌ای از موضوع‌های مختلف)، بیشترین تعداد مربوط به وبلاگ‌های سکولار بودند که بیشتر آنها نیز در خارج ایران قرار داشتند (Nafisi, 2008: 14-17).

ط) به چالش کشیده شدن انحصار دولت در اعمال خشونت: در گذشته فقط دولت‌ها حق مبادرت به جنگ و اعمال خشونت را داشتند، ولی امروزه فناوری اطلاعات با پدید آوردن فرصت‌های جدید برای اعمال خشونت موجب خروج انحصار آن از دست دولت‌ها شده است. این تغییر مربوط به ظهور حملات سایبری و جنگ اطلاعات است؛ یعنی هنگامی که از منابع سایبری برای تولید قدرت سخت یا خشونت نمادین استفاده شود (نای، ۱۳۸۹: ۴۵). موضوعیت یافتن این نوع خشونت به دلیل وابستگی و اتکای هرچه بیشتر دولت‌ها به زیرساخت‌های اطلاعاتی است که آنها را هرچه بیشتر در یک وضعیت آسیب‌پذیر نسبت به حملات سایبری قرار می‌دهد (Alberts & Papp, 1997: 147).

۶. سطوح چالش‌ساز فناوری‌های نوین برای امنیت ملی جمهوری اسلامی ایران

با عطف توجه به نیاز آینده کشور به توسعه فناوری اطلاعات و از سوی دیگر چالش‌ها و تنگناهای موجود در این ارتباط، می‌توان به دسته‌بندی چالش‌های موجود پرداخت. در بررسی و حیطه‌شناسی چالش‌های موجود، حوزه‌های چالش‌انگیز زیر به دست می‌آیند:

الف) چالش‌های قانونی

۱. ابهامات موجود درباره به رسمیت شناختن حقوق مالکیت‌های معنوی؛
۲. تعریف نشدن حقوق پدیدآورنده در قوانین؛

1. Kelly and Etling

۳. فقدان قانون جامع تجارت الکترونیک؛
۴. نقض قوانین درباره جرایم مرتبط با فناوری اطلاعات و ارتباطات؛
۵. تحریم‌های بین‌المللی و قوانین ناشی از آن در بهره‌مندی از توسعه فناوری اطلاعات؛
۶. به رسمیت شناخته نشدن امضای الکترونیکی؛
۷. فقدان ضمانت اجرایی برای حمایت از حقوق مصرف‌کننده.

ب) چالش‌های مربوط به ساختار بازارها
۱. موانع فعالیت بخش خصوصی؛
۲. ساختار سنتی بازارها.

ج) چالش‌های اجتماعی و فرهنگی
۱. سطح پایین دانش عمومی در زمینه فناوری اطلاعات و ارتباطات؛
۲. عدم اعتماد عمومی به امنیت اطلاعات.

د) چالش‌های مربوط به زیرساخت‌های نرم‌افزاری و سخت‌افزاری
۱. تناسب نداشتن آموزش‌های تخصصی با نیازهای جامعه؛
۲. استفاده نکردن از تجهیزات بومی؛
۳. ضعف زیرساخت‌های مخابراتی؛
۴. نبود استانداردهای مناسب در ارتباط با:
ـ استانداردهای تبادل اطلاعات؛
ـ استانداردهای کدگذاری کالا و خدمات؛
ـ استانداردهای کد مکان؛
ـ استانداردهای فونت فارسی؛
۵. نبود ابزارهای داد و ستد الکترونیکی و گسترش نیافتن بانکداری الکترونیکی (حسن بیگی، ۱۳۹۰: ۸ ـ ۱۰).

۷. مصادیق مرتبط با امنیت ملی جمهوری اسلامی ایران

تهدیدهای ماحصل فناوری‌های نوین، در پی از پای درآوردن اندیشه و تفکر جامعه هدف است تا حلقه‌های فکری و فرهنگی آن را سست و با بمباران خبری و تبلیغاتی به نظام سیاسی و اجتماعی حاکم تزلزل و بی‌ثباتی تزریق کند. جنگ رایانه‌ای و اینترنتی و راه‌اندازی شبکه‌های رادیویی و تلویزیونی و به طور کلی جنگ رسانه‌ای از مصادیق این امر و از مهم‌ترین اشکال جنگ نرم هستند. نظام بین‌الملل ۳۵ سال پس از وقوع انقلاب اسلامی به این نتیجه رسیده است که ضربه زدن به جمهوری اسلامی به شیوه سخت‌افزاری امکان‌پذیر نیست، اما جنگ نرم می‌تواند عاملی مهم برای تحقق خواسته‌های آنان باشد (رستمی و ممقانی، ۱۳۹۰: ۶۲ـ ۶۳). جمهوری اسلامی ایران تا کنون به دفعات در معرض حملات سایبری متعددی قرار گرفته است. ویروس‌هایی همچون استارس، استاکس‌نت، ناریلام و شعله آتش که هرکدام با هدف ضربه زدن به فعالیت‌های هسته‌ای ایران، بخش یا بخش‌هایی از زیرساخت‌های صنعتی کشور را آلوده کرده‌اند، از این دست بوده‌اند. ولی می‌توان گفت مهم‌ترین حمله جدی از این نوع در دهه ۸۰، ویروس استاکس‌نت[1] بوده است. این کرم رایانه‌ای یک حمله تروریستی محسوب می‌شد که نخستین بار در ژوئن ۲۰۱۰ شناسایی شد. از آنجا که هدف اصلی این حملات، فعالیت‌های هسته‌ای ایران بود و با توجه به حجم بالای طراحی و دانش تخصصی به کار رفته در تولید آن، نمی‌توانست از سوی یک هکر معمولی انجام شده باشد، بلکه در پس آن، عزمی دولتی و سیاسی وجود داشت، به همین دلیل بسیاری از کارشناسان منشأ آن را ایالات متحده و اسرائیل دانستند (بهمن، ۱۳۸۹: ۱۸)؛ زیرا برخی از تحلیلگران و افسران سابق ارتش آمریکا حملات سایبری به تأسیسات هسته‌ای ایران را مؤثرتر از بمباران آنها می‌پنداشتند (Alibright, Brannan, & Walrond, 2010). برخی متخصصان امنیتی در این حوزه معتقدند که این ویروس بزرگ‌ترین و سازمان‌یافته‌ترین حمله سایبری تاریخ را رقم زد و کد استاکس‌نت، طولانی‌ترین کدی است که تا کنون متخصصان امنیتی برای یک برنامه مخرب دیده‌اند؛ تا جایی که به گفته یوجنی کسپرسکی، بنیان‌گذار کمپانی امنیتی کسپرسکی در مسکو، استاکس‌نت همان بلایی را بر سر تأسیسات غنی‌سازی نطنز آورد که بمب‌های مهیب هسته‌ای بر سر هیروشیما و ناکازاکی آوردند، آن هم تنها با تکثیر قارچ‌گونه از طریق فلش‌های یواس‌بی.

1 . Stuxnet

۸. نمونه‌هایی از کارکردهای مفید فناوری‌های نوین برای امنیت ملی جمهوری اسلامی ایران

الف) ارتقای امنیت ملی

به طور واضح ایجاد امنیت ملی و در پی آن امنیت شهری نیازمند تلاش بسیار و به کارگیری مجموعه‌های متعدد است. اصلی‌ترین عنصر در امنیت، اطلاعات است و برای امنیت ملی این امر به معنی اطلاعات جغرافیایی است. در میان فناوری‌های نوین، فناوری GIS[1] در جمهوری اسلامی ایران توانسته است با آنالیز روابط جغرافیایی، انسان‌ها، ساختمان‌ها و منابع طبیعی به صورت فضایی، ابزار مناسبی برای پیاده‌سازی تلاش‌های امنیتی در روابط پیچیده ملی فراهم کند.

نباید فراموش کرد که اولین مسئولیت در طرح امنیت ملی، شناسایی تهدیدهای بالقوه و پیش‌بینی عوامل تهدیدکننده امنیت است. فناوری فضایی، ابزاری مناسب برای فراهم کردن اطلاعات لازم به منظور برنامه‌ریزی در مواردی همچون برنامه‌ریزی برای شرایط اضطراری، طرح مسیریابی، محافظت و دفاع، واکنش و کنترل است (رفیعیان، سرداری و پولادی،۱۳۸۷ : ۳).

ب) شبکه ملی دیتا

یکی از ویژگی‌های فناوری اطلاعات به ویژه اینترنت، امکان ساماندهی و تدارک سازمان‌یافته و از فواصل دور علیه اهداف از پیش تعیین‌شده است و به مهاجمان این امکان را می‌دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. شبکه ملی دیتا در ایران، علاوه بر اینکه موجب پنهان‌سازی نقاط ضعف موجود در زیرساخت‌های حیاتی کشور می‌شود با ایجاد ارتباط قوی باعث ارتقای واکنش‌های دفاعی یا ایجاد تأخیر در حملات سایبری شده است (حسن بیگی، ۱۳۹۰: ۳).

ج) ارتقای وفاق ملی

کار فناوری‌های نوین به خصوص رسانه‌های صوتی و تصویری در حفظ و تحکیم وفاق ملی جمهوری اسلامی ایران چه به لحاظ سخت‌افزاری و چه به لحاظ نرم‌افزاری، بالا بردن توان انتخاب جامعه، افزایش مشارکت، رقابت و پویایی شهروندان، درونی و نهادینه کردن نظام ارزشی و باورهای اعتقادی و معرفی سازوکارهای حل و فصل تعارض‌ها و چندگانگی‌های فرهنگی و اجتماعی است. در حقیقت وسایل ارتباط جمعی

1 . Geographic Information System

می‌توانند به برقراری و استحکام رابطه میان تنوع و وحدت یا تمایز و یکپارچگی مدد رسانند تا وفاق ملی و در نهایت امنیت ملی پایدار بماند (شاه‌محمدی، ۱۳۹۰: ۴۶).

د) دولت الکترونیکی

دولت الکترونیکی، به عنوان مهم‌ترین کاربرد در استفاده از فناوری‌های نوین در ایران است. دولت الکترونیکی تمهیداتی را برای کارکنان دولت فراهم می‌کند که با در خدمت گرفتن فناوری اطلاعات و ارتباطات، بتوانند با دقت بیشتر و سریع‌تر به صورت استاندارد وظایف محوله را به بهترین شکل انجام دهند.

نوع نگرش به دولت الکترونیکی کاملاً با روال‌های سنتی متفاوت است. در روش‌های سنتی، اطلاعات عموماً روی کاغذ نگهداری می‌شود و روش‌های ایمن‌سازی نقل و انتقال و نگهداری اطلاعات کاملاً مشخص و نسبتاً آسان است؛ اما در روش الکترونیکی که اطلاعات روی سرورها قرار می‌گیرند تا در اختیار کاربران قرار گیرند، مکانیزم نگهداری ایمن اطلاعات بسیار مهم و حیاتی است (موحدی، ۱۳۸۶: ۲۵۴).

۹. پیشینه تحقیق

الف) پیشینه داخلی

ـ خلیلی و نورعلی وند (۱۳۹۱) در تحقیقی که انجام داده‌اند، معتقدند فضای سایبر مفهوم امنیت را تغییر داده است و امنیت ملی دیگر صرفاً در ارتباط با مرزهای جغرافیایی نیست، بلکه افت کیفیت شهروندان نوعی تهدید امنیت ملی است (خلیلی پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۶۸).

ـ قدسی (۱۳۹۲) در تحقیق خود به بررسی تأثیر فضای مجازی بر امنیت ملی در حوزه‌های اجتماعی‌ـ فرهنگی، سیاسی، امنیت و روان‌شناختی پرداخته و معتقد است فضای مجازی مانند شمشیری دولبه از یک سو ساختارهای فرهنگی، اجتماعی و امنیتی ملت‌ها را با تهدید متوجه ساخته و از سوی دیگر، فرصت‌های ارزشمندی را برای معرفی قابلیت‌های جوامع فراهم کرده است (قدسی، ۱۳۹۲: ۱۵۰).

ـ کریمی و کیان‌خواه (۱۳۹۴) به بررسی چالش‌های مربوط به استفاده از تکنولوژی‌های غیربومی به ویژه اینترنت اشیا بر امنیت ملی پرداخته و معتقدند باید با درک صحیح چالش‌های آینده، راهبردهایی را در شکل‌دهی به قدرت دورن‌زای سایبری اتخاذ کرد (کریمی قهرودی و کیان‌خواه، ۱۳۹۴: ۸۳).

ـ سلطانی‌نژاد و اسدی‌نژاد (۱۳۹۲) معتقدند فناوری اطلاعات در دهه ۸۰ تهدیدی جدی را متوجه امنیت ملی نساخته است؛ با این حال آسیب‌پذیری کشور را در برخی مؤلفه‌ها برجسته کرده است (سلطانی‌نژاد و اسدی‌نژاد، ۱۳۹۲: ۳۵ـ ۷۰).

ـ موحدی صفت (۱۳۸۶) معتقد است چنانچه در استفاده از فناوری اطلاعات و ارتباطات، امنیت تأمین نشود، فرصت به تهدید تبدیل می‌شود و صدمات جبران‌ناپذیری دارد (موحدی صفت، ۱۳۸۶: ۲۴۵ـ ۲۹۰).

ـ بصیری (۱۳۸۲) معتقد است پس از فروپاشی شوروی سابق و پایان جنگ سرد در این مفهوم نیز تغییر ایجاد شد؛ یعنی با توجه به گسترش ارتباطات ـ اطلاعات و مسئله دهکده جهانی، مفهوم امنیت ملی از دو شکل قبلی، ضمن حفظ نسبی ابعاد آن، به سوی توان فرهنگی‌ـ ارتباطی‌ـ اطلاعاتی سوق یافت (بصیری، ۱۳۸۲: ۶۹ـ ۸۰).

ـ حسن بیگی (۱۳۹۰) به بررسی چالش‌های فراروی استفاده از شبکه ملی دیتا و تهدیدهای متوجه امنیت ملی پرداخته و معتقد است جمهوری اسلامی ایران باید اقدام به طراحی استراتژی در ارتباط با فناوری اطلاعات و بهره‌مندی از این فضا کند و بر اساس آن نسبت به پیاده‌سازی شبکه ملی دیتا اقدام کند (حسن‌بیگی، ۱۳۹۰: ۴۷ـ ۷۵).

ـ شاه محمدی (۱۳۹۰) در تحقیقی که انجام داده، به بررسی نقش رسانه در امنیت ملی پرداخته و معتقد است شرایط ویژه زمانی، جهانی و ملی، رویکردها و نگرش‌های خلاقانه روز را طلب می‌کند؛ یعنی نگاه‌ها و راه‌حل‌هایی که به آثار و عوارض منفی و مثبت رسانه‌های جمعی توجه کند (شاه‌محمدی، ۱۳۹۰: ۴۳ـ ۵۷).

ـ رستمی و ممقانی (۱۳۹۰) به آینده‌پژوهی فضای رسانه و امنیت ملی جمهوری اسلامی ایران پرداختند و معتقدند کشورهایی که هنجار تمایز از هنجارهای حاکم بر عرصه بین‌المللی دارند، بیشترین مواجهه را با رسانه‌های غربی خواهند داشت (رستمی و ممقانی، ۱۳۹۰: ۵۷ـ ۷۴).

ـ ولوی و همکاران (۱۳۹۱) در تحقیق خود به استخراج اولویت‌های علم و فناوری در حوزه دفاع، امنیت ملی و سیاست خارجی پرداختند و معتقدند باید اولویت‌های پژوهشی و فناوری هر بخش کشور مشخص شود و پس از تعیین این اولویت‌ها، دستگاه‌های مسئول موظف هستند برنامه‌های پژوهشی و توسعه فناوری خود را تا حد ممکن در این راستا تعریف کنند (ولوی، طرهانی و مجردی، ۱۳۹۱: ۲۷ـ۶۵).

ـ آقایی و ثانی‌آبادی (۱۳۹۰) به تأثیر انقلاب اطلاعات بر امنیت ملی پرداختند و در تحقیق خود ضمن شناسایی نظریات مطرح‌شده در متون روابط بین‌الملل، دیدگاه‌های این نظریات به مقوله انقلاب اطلاعات را بیان کردند (آقایی و ثانی‌آبادی، ۱۳۹۰: ۲۳ـ۳۷).

ـ صادقیان (۱۳۸۷) در تحقیقی به نقش کارکردی رسانه‌ها در امنیت ملی و عمومی پرداخته و معتقد است برخلاف تصور برخی، رسانه‌ها در تقابل با امنیت عمومی و ملی نیستند، بلکه مکمل و مهم‌ترین عامل تقویت‌کننده امنیت ملی و عمومی هستند (صادقیان، ۱۳۸۷: ۱۶۵ـ ۱۸۰).

ب) پیشینه خارجی

ـ اریکسون و گیسپیارو (۲۰۰۶)[1] در تحقیقی که انجام داده‌اند، معتقدند از آنجا که امروزه توسعه فناوری‌های ارتباطی و اطلاعاتی از قبیل اینترنت، ایمیل، ماهواره و تلفن همراه با سرعتی درخور توجه انجام می‌گیرد، بهتر شدن یا بدتر شدن جهان کاملاً به فناوری‌های نوین بستگی دارد (Ericsson & Gismpiaro, 2006: 221).

ـ از نظر رونالد دیبرت (۲۰۰۷)،[2] پیامد فناوری اطلاعاتی یا فرافناوری بر عرصه سیاست بین‌الملل عبارت‌اند از: افزایش نقش بازیگران غیردولتی، پیامدهای اجتماعی‌ـ سیاسی آن بر مفاهیم بین‌الملل و در نهایت بازتعریف هویت بازیگران بین‌المللی (Muftuler, 2007: 131).

ـ بیل کولمان (۲۰۰۰)[3] نیز معتقد است ظهور و توسعه شبکه‌های اطلاعاتی، الکترونیک، اجتماعی و رسانه‌ای نشان‌دهنده دورانی تازه و پیچیده‌تر در روابط بین‌الملل و بیانگر آن است که در آغاز سومین انقلاب صنعتی هستیم که با توسعه فناوری‌های دیجیتالی ایجاد شده است (Killing & Others, 2000: 21).

ـ به نظر هررا (۲۰۰۳)،[4] فناوری‌ها از جمله فناوری اطلاعاتی در کشاکش‌های اجتماعی و سیاسی میان بازیگران به وجود آمده‌اند و در مراحل بعد، جدای از این منازعات و نیروهای اجتماعی به عنوان پدیده‌هایی مستقل و دارای قدرت علّی و تأثیرگذار بر روابط، تعاملات، سیاست و امنیت آنها مطرح می‌شوند (Herrera, 2003: 561).

ـ سیوونن و هنریکی (۱۹۹۵)[5] در تحقیقی که روی امنیت ملی کشورهای مختلف انجام داده‌اند، معتقدند روندهایی که از فناوری‌های نوین نشئت می‌گیرند، بی‌شک بیشترین تأثیر را در شکل‌دهی به بخش‌هایی از آینده یک کشور خواهند داشت (Sivonen & Henrikki, 2007: 4).

1 . Ericsson & Gismpiaro
2 . Ronald Deibert
3 . Bill Coleman
4 . Herrera
5 . Sivonen &Henrikki

ـ اسکولینکوف (۱۹۹۵)[1] تلاش آمریکا برای یافتن سیاست‌هایی برای توسعه توانمندی‌های فناورانه و حفظ برتری‌اش نسبت به رشد ژاپن در این دهه را نشئت‌گرفته از استفاده بیشتر آمریکا از علم و فناوری در تمامی حوزه‌های امنیت ملی آن کشور می‌داند (Skolnikoff, 1995: 2).

ـ دیک (۲۰۰۳)[2] در تحقیقی که روی چندین کشور (استرالیا، انگلستان، روسیه و ایالات متحده) انجام داده، به بررسی تعامل علم و فناوری در آن کشورها با حوزه‌های دفاع، امنیت ملی و سیاست خارجی پرداخته و هریک از کشورهای یادشده را از بعدی خاص مورد بررسی قرار داده است (Dick, 2003: 3-43).

ـ دولت استرالیا (۲۰۰۹) در تحقیقی به بررسی تعامل فناوری با بخش امنیت ملی در کشورهای استرالیا و آمریکا و نقشی که علم و فناوری در این کشورها در امنیت ملی ایفا می‌کند، پرداخته و به این نتیجه رسیده است که امنیت ملی این دو کشور به شدت تحت تأثیر علم و فناوری است (Australian Goverment, 2009: 1-120).

ـ مؤسسه رند (۲۰۰۹)[3] در تحقیقی که در روسیه انجام داده به بررسی نتایج حاصل از کنش متقابل بین دو حوزه «سیاست خارجی» و «علم و فناوری» به ویژه در روسیه پرداخته و امنیت روسیه را متأثر از علم و فناوری دانسته است (Oriker, Crane, & H. schwartez, 2009: 1-194).

ـ در تحقیقی که مؤسسه Russia International S &T Center (۲۰۰۷) در روسیه انجام داده است، با بررسی راهبردها و ابزار حوزه سیاست خارجی در راستای توسعه علم و فناوری، به تشریح راهبردهای این حوزه پرداخته است (Internationa Science &Technology, 2007).

ـ گلدمن (۲۰۰۵)[4] در تحقیقی نظریات واقع‌گرایان جنگ اطلاعاتی را بررسی کرده و معتقد است ایالات متحده با استفاده از فناوری‌های اطلاعاتی و انقلاب در امور نظامی توانسته است به جایگاه هژمونیک در نظام بین‌الملل دست یابد (Goldman, 2005).

ـ گلدستین (۲۰۰۶)[5] در تحقیق خود به حملات ۱۱ سپتامبر اشاره کرده و معتقد است تروریست‌ها با استفاده از فناوری‌های اطلاعاتی توانستند امنیت ایالات متحده آمریکا را به خطر بیندازند (Golstien, 2006).

1 . Skolnikoff
2 . Dick
3 . Rand
4 . Goldman
5 . Goldstein

ـ بوزان[1] و همکارانش (۱۹۹۸) در تحقیق خود برداشت‌های سنتی و تقلیل‌گرایانه از امنیت را نقد کرده و مفهوم «امنیت وسعت داده‌شده» را در مقابله با «امنیت محدود» مد نظر واقع‌گرایان قرار داده‌اند (Buzan, Weaver, & Wilde, 1998: 1-239).

۱۰. سؤال‌های تحقیق

سؤال اصلی این تحقیق عبارت است از:

ـ تأثیرات استفاده از فناوری‌های نوین بر مدیریت امنیت جمهوری اسلامی ایران چیست؟

ـ چالش‌های نوین امنیت ملی جمهوری اسلامی ایران متأثر از گسترش فناوری‌های نوین و فناوری‌های مرتبط با آن کدام است؟

ـ فناوری‌های نوین، چه فرصتی برای امنیت ملی جمهوری اسلامی ایران فراهم کرده است؟

همچنین سؤال‌های فرعی این پژوهش عبارت است از: مفهوم فناوری‌های نوین و خدمات شکل‌گرفته از آن چیست؟

۱۱. روش تحقیق

پژوهش حاضر به دنبال تبیین نقش (چالش‌ها، فرصت‌ها و تأثیرات) فناوری‌های نوین در مدیریت امنیت ملی است و بر این اساس باید گفت پژوهش به شیوه توصیفی و از نوع تحلیل اسنادی انجام شده است.

۱۲. جامعه و نمونه تحقیق

با توجه به اینکه در پژوهش حاضر همه منابع و مراجع موجود فیش‌برداری شده و در راستای هدف پژوهش مورد استفاده قرار گرفته است، نمونه‌گیری انجام نشده و همه منابع و مراجع در دسترس بررسی و تحلیل شده‌اند.

نتیجه‌گیری

فناوری‌های نوین به سرعت در حال گسترش‌اند. اینترنت با نفوذ در همه شئون زندگی انسان از حالات شخصی و فردی تا تعاملات جمعی، اجتماعی، اقتصادی، سیاسی و

1 . Buzan

فرهنگی در حال خلق دنیایی جدید برای انسان است. فناوری‌های نوین در کنار مزایای زیادی که دارد، بدان علت که طراحان و تولیدکنندگان آن متعلق به کشورهایی دارای فرهنگ و ایدئولوژی متفاوت با فرهنگ انقلاب اسلامی و همچنین کشورهایی هستند که با جمهوری اسلامی ایران خصومت دارند، چالش‌های جدیدی را متوجه امنیت ملی جمهوری اسلامی و متولیان آن خواهند کرد. این چالش‌ها و تهدیدها در موضوعاتی همچون مردم و سبک زندگی، حاکمیت و قلمرو جغرافیایی، تغییر نگرش به زندگی و تحول سبک زندگی دینی به سمت سبک زندگی غربی تا اشراف کشورهای متخاصم بر رفتار و تعاملات فردی و کاهش حفاظت از سرمایه‌های ملی خواهد بود. فناوری‌های نوین و صنایع وابسته به آن، یکی از مهم‌ترین و تأثیرگذارترین منابع قدرت در هزاره سوم هستند. این تأثیرگذاری را از چند جهت می‌توان ارزیابی کرد:

نخست، مفهوم امنیت؛ دیگر نمی‌توان امنیت ملی را همانند گذشته در ارتباط با مسائل نظامی و مرزهای داخلی و خارجی تعریف کرد، بلکه امروزه خطر افت زندگی شهروندان نوعی تهدید برای امنیت ملی محسوب می‌شود.

دوم، از میان رفتن بعد جغرافیایی در تهدیدهای سایبری؛ در گذشته، تهدیدهای نظامی از محل جغرافیایی خاصی برخوردار بودند؛ در نتیجه، مقابله با آن دست‌کم از جهت شناسایی، کار چندان دشواری نبود.

سوم، گستردگی آسیب‌پذیری‌های ناشی از فناوری‌های نوین؛ این تهدیدها پراکنده، چند بعدی و چند سویه‌اند و چون در ارتباط با شبکه‌های ارتباطی و زیرساخت‌های حساس هستند، سطح آسیب‌رسانی آنها بسیار زیاد است.

چهارم، چون امنیت در عصر اطلاعات صرفاً دولت‌محور نیست، رویکردهای مختلف نظری در روابط بین‌الملل که به طور عمده بر مبنای دولت‌محوری به ساختاربندی نظریات خود پرداخته‌اند، یا به راحتی از کنار این تهدیدها گذشته‌اند یا در تحلیل‌های خود با سردرگمی مواجه شده‌اند.

پنجم، موضوعات مربوط به مزیت‌های فناوری‌های نوین برای امنیت ملی کشورها که متأسفانه در اغلب کتب و منابع تألیف‌شده به آن پرداخته نشده است؛ در حالی که فرصت‌های این ابزار برای کشورهای در حال توسعه همچون ایران، کم نیست و مدیران امنیت ملی کشور می‌توانند از آن استفاده کنند.

ارائه راهکار

پیش از تدوین راهکارها، باید به این نکته توجه کرد که هرچند تهدیدها و چالش‌های یادشده، ناشی از فناوری‌های نوین است، ولی راه‌حل‌های مقابله با آنها را نمی‌توان تنها به حوزه این فناوری‌ها محدود کرد، بلکه اقدام در حوزه‌های غیرفناورانه همچون مدیریت، اقتصاد، جامعه و فرهنگ نیز هست. با توجه به این نکته، در ادامه برخی راهکارها ارائه می‌شود:

۱. تقویت بخش خصوصی: باید پذیرفت تنها راه توسعه فناوری اطلاعات، از مسیر تقویت بخش خصوصی است. البته خصوصی‌سازی به معنای توسعه این صنعت صرفاً براساس نیازهای بازار نیست، بلکه به دلیل محدود بودن توانمندی کشورهای در حال توسعه، حمایت دولت- نه تصدی‌گری- در برخی حوزه‌ها ضرورت دارد. دولت باید تنها نقش تعادل‌بخشی داشته باشد و به سیاست‌گذاری و نظارت بپردازد.

۲. توسعه اقتصادی: فناوری اطلاعات با کاهش هزینه‌ها، افزایش کیفیت و ایجاد ارزش افزوده، فرصت‌های بسیاری را برای توسعه اقتصادی ایجاد می‌کند. برای نمونه تجارت الکترونیک می‌تواند با توسعه و گسترش روابط عرضه و تقاضا هزینه‌ها را کاهش و کیفیت تولید را افزایش دهد. جمهوری اسلامی ایران نیز باید از طریق پیوند با پیشرفت‌های تکنولوژیک، زمینه‌های حضور قوی خود را در آینده این صنعت فراهم سازد.

۳. تقویت امنیت نرم: امروزه در راستای جنگ نرم و قدرت نرم، صحبت از امنیت نرم است. امنیت نرم اشاره به امنیتی دارد که از بازیگران در برابر صدمات و خطرها به گونه‌ای ملایم و ناملموس حراست می‌کند. یکی از رموز وقوع انقلاب اسلامی نیز انتشار پیام نرم صلح و عدالت بیرون از مرزهای خود بود؛ بنابراین در سده ۲۱ نیز قدرت نرم و پیام نرم باید رویکرد محوری نظام باشد.

۴. ایجاد توازن در ابعاد هویتی: این راهکار در واقع در جهت حفظ و تقویت انسجام ملی است. هرچند ایران کشوری قومیتی است، اقلیت‌های ساکن در ایران اساساً ایرانی هستند؛ به این ترتیب در برخورد با آنها نباید به دید اقلیت رفتار شود. سازنده‌ترین راه، شریک کردن گروه‌های قومی در قدرت است.

۵. تقویت دیپلماسی عمومی: فراوانی اطلاعات در عصر کنونی موجب فقر توجه و تمرکز بر اطلاعاتی خاص می‌شود. همین عامل منبع قدرتی را برای آنهایی که می‌توانند به ما بگویند توجه‌مان را کجا متمرکز سازیم، ایجاد می‌کند. ایران نیز باید خود را به نوع نوین دیپلماسی نفوذ برای تأثیرگذاری یا تغییر فضای رسانه‌ای خارج از مرزها مجهز سازد.

۶. حفاظت از زیرساخت‌ها: هر چند ما در عمل با یک حمله سایبری جدی روبه‌رو نشده‌ایم، ولی انگیزه‌ها و توانمندی‌های وسیعی برای بهره‌برداری از آسیب‌پذیری زیرساخت‌ها وجود دارد که تدبیری همه‌جانبه برای محافظت از زیرساخت‌ها را ضروری می‌سازد.

۷. فرهنگ‌سازی برای استفاده بهینه از فضای مجازی: دولت باید فرهنگ استفاده بهینه از فضای مجازی و فناوری‌های نوین را با کمک رسانه‌های ملی و جراید در افکار عمومی نهادینه کند. متأسفانه کشور ما در زمینه استفاده مناسب از دانش و فناوری‌های بیگانه جدید، همواره با مشکلاتی روبه‌رو بوده است که جا دارد برای فناوری‌هایی که حداقل در آینده با آنها روبه‌رو خواهیم شد، برنامه‌ریزی مناسب و دقیق داشته باشیم که این امر نیاز به توجه برنامه‌ریزان فرهنگی کشور دارد.

منابع فارسی

ـ آقایی، د. و ثانی آبادی، ا (۱۳۹۰)، «تأثیر انقلاب اطلاعات بر امنیت ملی از منظر نظریه‌های روابط بین‌الملل»، **فصلنامه سیاست**.

ـ ایران، م. ت. (۱۳۸۲)، **بررسی فعالیت‌های داخلی و خارجی مرتبط با امنیت اطلاعات کشور**، تهران: مرکز تحقیقات مخابرات ایران.

ـ بابایی، م. و فهیمی‌فر، س (۱۳۹۱)، «ویژگی‌های رسانه‌های نوین و الگوهای ارتباطی»، **فصلنامه مطالعات ملی کتابداری و سازماندهی اطلاعات**.

ـ بصیری، م. (۱۳۸۲)، «تحولات مفهوم امنیت ملی»، **خاورمیانه**.

ـ بوزان، ب. (۱۳۷۸)، **مردم، دولت‌ها و هراس**، تهران: پژوهشکده مطالعات راهبردی.

ـ بهمن، ش (۱۳۸۹)، «جنگ سایبری آمریکا و رژیم صهیونیستی علیه ایران»، **روزنامه همشهری**، ش ۱۸.

ـ پورسعید، ف. (۱۳۸۸)، «بازتولید گفتمانی؛ راهبرد استقرار امنیت نرم در جامعه ایرانی»، **فصنامه مطالعات راهبردی**، ش ۱۳۵.

ـ تاجیک، م. (۱۳۸۱)، **مقدمه‌ای بر استراتژی‌های امنیت ملی**، تهران: فرهنگ گفتمان.

ـ تافلر، آ. (۱۳۷۶)، **به سوی تمدن جدید**، تهران: انتشارات سیمرغ.

ـ حسن بیگی، ا. (۱۳۹۰)، «توسعه شبکه ملی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملی»، **فصلنامه مطالعات مدیریت**.

ـ خلیفه، ق.ا. (۱۳۹۱)، «کاربرد تکنولوژی‌های رایانه‌ای در افزایش مهارت‌های روانی‌ـ حرکتی»، **فصلنامه راهبردهای آموزش**.

ـ خلیلی‌پور رکن‌آبادی، ع. و نورعلی وند، ی. (۱۳۹۱)، «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، **فصنامه مطالعات راهبردی**، ش۱۶۸.

ـ رحمت الهی، ح. (۱۳۸۴)، «جهانی شدن و تأثیر آن بر هویت‌های قومی و ملی»، **اندیشه‌های حقوقی**.

ـ رستمی، ف. و ممقانی، ج. (۱۳۹۰)، «آینده‌پژوهی فضای رسانه و امنیت ملی جمهوری اسلامی ایران»، **فصلنامه آفاق امنیت**.
ـ رضاییان، ع. (۱۳۸۰)، **اصول مدیریت**، تهران: سمت.
ـ رفیعیان، م.، سرداری، م. و پولادی، ر. (۲۰۰۷)، «نقش فناوری اطلاعات جغرافیایی در کنترل و توسعه امنیت شهری»، First Coference of Urban GIS. Iran: Shomal uiversity.
ـ روزنا، ج. و دیگران (۱۳۹۰)، **انقلاب اطلاعات، امنیت و فناوری‌های جدید**، تهران: پژوهشکده مطالعات راهبردی.
ـ سلطانی نژاد، ا. و اسدی نژاد، ا. (۱۳۹۲)، «تأثیر فناوری اطلاعات و ارتباطات بر امنیت ملی جمهوری اسلامی ایران در دهه ۸۰»، **پژوهشنامه علوم سیاسی**، ش ۸۰.
ـ شاه محمدی، ع. (۱۳۹۰)، «بررسی نقش رسانه‌ها در امنیت ملی»، **فصلنامه مطالعات رسانه‌ای**.
ـ شعرباف، ج. (۱۳۹۰)، « امنیت ملی آمریکا؛ مفهوم سیّال، ماهیتی ثابت»، **فصلنامه مطالعات جهان**.
ـ صادقیان، س. (۱۳۸۷)، «بررسی نقش کارکردی رسانه‌ها در امنیت ملی و عمومی»، **فصلنامه دانش انتظامی**.
ـ صالحی امیری، س.، انتخابی، ش. و سلطانی فر، م. (۱۳۸۷)، **دیپلماسی رسانه‌ای**، تهران: گروه پژوهش‌های فرهنگی و اجتماعی مجمع تشخیص مصلحت.
ـ عبداله خانی، ع. (۱۳۸۲)، **نظریه‌های امنیت؛ مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی**، تهران: مؤسسه مطالعات و تحقیقات ابرار معاصر تهران.
ـ عطارزاده، م. (۱۳۹۲)، «تأثیر رویکرد جدید مفهوم امنیت بر امنیت ملی جمهوری اسلامی ایران»، **فصلنامه مطالعات راهبردی**.
ـ علاقه‌بند، ع. (۱۳۷۴)، **مقدمات مدیریت آموزشی**، تهران: بعثت.
ـ قدسی، ا. (۱۳۹۲)، «تأثیر فضای مجازی بر امنیت ملی جمهوری اسلامی ایران و ارائه راهبرد»، **مجله راهبرد دفاعی**.
ـ کرامر، ف.، استار، ا. و ونتز، ل. (۱۳۹۴)، **قدرت سایبری و امنیت ملی**، تهران: مؤسسه چاپ و انتشارات دانشکده اطلاعات.
ـ کریمی قهرودی، م. و کیان خواه، ا. (۱۳۹۴)، «چالش‌آفرینی اینترنت اشیا بر ارکان امنیت ملی کشور»، **فصلنامه امنیت ملی**، ش۸۳.
ـ کونتز، ه.، اودائل، س. و ویهریخ، ه. (۱۳۷۰)، **اصول مدیریت**، تهران: مرکز آموزش مدیریت دولتی.
ـ لطف الهی حقی، م. (۱۳۸۹)، «تکنولوژی در سازمان»، **فصلنامه عصر مدیریت**، ش۸۳.
ـ موحدی صفت، م. (۱۳۸۶)، «امنیت ملی در فضای سایبر، فرصت‌ها و تهدیدها با تأکید

بر استقرار دولت الکترونیکی»، **فصلنامه مطالعات دفاعی استراتژیک**.
ـ ناجی، س. (۱۳۹۲)، «روح تکنولوژی نوین و جایگاه تفکر در مدارس»، **فصلنامه تفکر و کودک**.
ـ نای، ج. (۱۳۸۹)، **قدرت نرم، ابزارهای موفقیت در سیاست بین‌الملل**، تهران: دانشگاه امام صادق(ع).
ـ نصیری، ح. (۱۳۸۴)، «امنیت ملی پایدار»، **فصلنامه اطلاعات سیاسی و اقتصادی**.
ـ نقیب‌زاده، ا. (۱۳۸۸)، **تأثیر فرهنگ ملی بر سیاست خارجی جمهوری اسلامی ایران**، تهران: دانشگاه امام صادق(ع).
ـ نیک سیر، ف. (۱۳۸۴)، **راهنمای فراسکاتی برای ارزیابی فعالیت‌های تحقیق و توسعه**، تهران: مرکز تحقیقات سیاست علمی کشور.
ـ وحیدی، م. ا. (۱۳۸۶)، «فراتکنولوژی و تحول مفهوم قدرت در روابط بین‌الملل»، **مطالعات راهبردی**.
ـ ولوی، م.، طرهانی، ف. و مجردی، س. (۱۳۹۱)، «استخراج اولویت‌های علم و فناوری در حوزه دفاع؛ امنیت ملی و سیاست خارجی»، **فصلنامه راهبرد دفاعی**.
ـ هالپین و دیگران (۱۳۸۹)، **جنگ سایبر؛ جنگ اینترنتی و انقلاب در امور نظامی**، تهران: مرکز پژوهش‌های مجلس.
ـ یزدان فام، م. (۱۳۸۶)، «دگرگون در نظریه‌ها و مفهوم امنیت ملی»، **فصلنامه مطالعات راهبردی**.

منابع لاتین

- Alberts & Papp, (1997), ***Information Age Anthology: National Security Implications of the Information Age***, US: National Defene University by NDU press and DOD CCRP Publications.

- Alibright, Brannan, P & ,.Walrond, C. (December 2010),"Did Stuxnet Take out 1000 Centrifuges at the Natanz Enrichment Plant", in http://isis-online.org

- Buzan, B., Weaver, O & ,.Wilde, J. (1998), ***Security: A New Framework for Analysis***, London: Lynee Rienner.

- Dick, C. J. (2003),"The Future of Conflict: Looking out to 2020", ***Defence Academy of the United Kingdom***43-3..

- Donnelly, J. (1975), ***Fundamentals of Management***, Texas: Bussiness Publication.

- Dumbrell, J.(2007),***The Bush Administration***,US: Durban University.

- Ericsson, J & ,.Gismpiaro, G. (2006), The Information Revolution, Security and International Relations:(IR) Relevant Theory?", ***International Plitical Science Review***.

- Evans, G. & New Ham, J. (1998), ***The Penguin Dictionary of International Relations***, London: Penguin Books.

- Goldman, E. (2005), ***Information and Revolution in Military Affairs***, London: Rout Ledge.

- Golstien, J. (2006), "Effects of the Information Revolution on International Relations", duke.edu.

- Goverment, A. (2009)," The National Science and Innvation Strategy", ***Department of the Prime Minister and Cabinet***.

- Herrera, G. L. (2003),"Technology and International Systems", ***Millennium: Journals of International Studies***.

- Killing, R. & Others (2000), "Learning from Social Informations", ***Critical Security Studies: Concepts and Cases***, www.slis.indiana.edu.M.C.Williams.

- Mazarr, J. M. (2005), "Information Technology and World Politics", ***Hampshire***.

- Muftuler, M. (2007),"Information Societies, New Terrorism: It's Impact on International Politics", Politico: www.uluslararasi.com.

- Nafisi, A. (2008), ***Blogging Outside Iran: A Tool for Internal Democratic Change, Thesis Advisor***, US: Unversity of Washington Departement of Communication Honors Program.

- Oriker, O., Crane, K & ,.H. Schwartez, l. (2009),"Russia Foreign Policy: Source and Implications", ***Santa Monica***.

- Price, E.M. (2002), "Media and Sovereignty: The Global Information Revoulation and It's Challenge for State Power", USA: MAssachusetts Institue of Technology.

- Rahimi, B. (2003),"Cyber Dissent: The Internet in Revolutionary Iran", ***Middle East Review of international Affairs***.

- Riterz, G. (2007),"The Blackwel Companion to Globalization", ***Middle East Review of International Affairs*** , Blackwell Publishing.

- Rothkopt, D. (1998),"Cyber Politics: The Changing Nature of Power in the Information Age", ***Journals of International Affairs***.

- Sarkisian, S., Williams, J. & Cimbala, S. (2008), ***US National Security***, London: Lynne Rienner.

- Sivonen, P. & Henrikki, H. (2007), "Predictions Regarding International Actors up to the Year 2030", ***Ministry od Defence***.

- Skolnikoff, E . (1995), "Evoving US Science and Technology Policy in a Changing International Environment", ***Science and Public Policy,*** 2.

- Technology, I. S. (2007), "Russia: International Science& Technology", http://www.nti.org.