

# تأثیر فناوری اطلاعات و ارتباطات بر امنیت ملی جمهوری اسلامی ایران در دهه ۱۳۸۰

\* احمد سلطانی نژاد

\*\* مسعود موسوی شفقانی

\*\*\* الهام اسدی نژاد

## چکیده

ضریب نفوذ فناوری اطلاعات و ارتباطات در ایران، در دهه ۱۳۸۰ افزایش چشمگیری داشته به طوری که به متغیر مستقلی برای بیان برخی تغییرات سیاسی و اجتماعی تبدیل شده است. هدف از این مقاله، بررسی تأثیر اینترنت و تلفن همراه به عنوان دو نماد اصلی در عصر فناوری اطلاعات بر امنیت ملی جمهوری اسلامی ایران در دهه ۱۳۸۰ است. بررسی یادشده با

---

\* استادیار گروه روابط بین الملل دانشگاه تربیت مدرس (soltani@modares.ac.ir)  
\*\* استادیار گروه روابط بین الملل دانشگاه تربیت مدرس (shafae@modares.ac.ir)  
\*\*\* کارشناسی ارشد روابط بین الملل دانشگاه تربیت مدرس (asadinezhad.elham@yahoo.com)

تاریخ پذیرش: ۱۳۹۱/۸/۵

تاریخ دریافت: ۱۳۹۱/۳/۲۰

پژوهشنامه علوم سیاسی، سال هشتم، شماره دوم، بهار ۱۳۹۲، صص ۷۹-۱۱۲.

بهره‌گیری از نظریه آشوب جیمز روزنا در قالب سه پارامتر خرد، کلان و تلفیق (خرد - کلان) انجام می‌شود. فرضیه اصلی آن است که هرچند تأثیر تحولات مربوط به این فناوری‌ها تهدید جدی‌ای را در بر نداشته ولی آسیب‌پذیری کشور در برابر موجی از تغییرات را نشان می‌دهد. اختلاف میان دولت و گروهی از مردم، افزایش فعالیت گروه‌ها و بازیگران خارجی علیه دولت، تهدید ارزش‌های دینی و تضعیف انسجام ملی می‌تواند در این راستا قابل ذکر باشد که راهکارهایی اساسی و نه برخورد‌های مقطعی را می‌طلبد.

واژگان کلیدی: فناوری اطلاعات، اینترنت، امنیت ملی جمهوری اسلامی ایران، نظریه آشوب.

### مقدمه

امروزه عامل اطلاعات چنان زندگی بشر را متحول ساخته و الگوی گسستی را در بنیان اقتصاد، جامعه و فرهنگ پدید آورده که از آن به عنوان شاخص مستقلی برای تعریف دور تازه‌ای در تاریخ تحولات بشر یاد می‌شود. البته ورود به دوره جدید، به معنای ازمیان رفتن کامل نظم گذشته نیست؛ دنیای جدید با جهان قدیم هم‌پوشانی داشته و در آن قدرت همچنان به نهادهای مبتنی بر جغرافیا وابسته است (روزنا و سینگ، ۱۳۹۱: ۳۷). این نکته بیانگر تداوم اهمیت دولت‌های سرزمینی و توجه شدید سیاسی به امنیت ملی است (بوزان، ۱۳۷۸: ۲۷) زیرا امنیت ملی به موجودیت و حیات یک کشور باز می‌گردد. با توجه به اهمیت این مسئله، تمرکز اصلی در اینجا بر تأثیر فناوری‌های جدید بر امنیت ملی جمهوری اسلامی ایران است زیرا جامعه ما به عنوان یک جامعه جوان دائماً در صدد تجربه و تلاش در راه دستیابی به امکاناتی برای ارتقای سطح توسعه و افزایش ارتباطات جهانی خود بوده است، از این رو نیازمند درک بهتر و عمیق‌تر از فناوری‌های نوین در جهت پیشرفت و تکامل جامعه است تا با بینشی روشن و به دور از بدبینی مفرط به بهره‌برداری از فرصت‌ها و مقابله با تهدیدها بپردازد.

در میان فناوری‌های متعدد، تمرکز اصلی روی اینترنت و تلفن همراه است؛ به دلیل ضریب نفوذ بالای این دو فناوری در ایران<sup>(۱)</sup> و همچنین به دلیل کیفیت و ویژگی‌های منحصر به فردی که آنها را از سایر فناوری‌های پیش از خود مجزا و به نماد عصر اطلاعات تبدیل می‌سازد. به عنوان نمونه عدم تمرکز، تعاملی بودن و امکان مراوده دوسویه و غیره از طریق اینترنت و تحرک، هزینه اندک، کاربرد آسان و قابلیت اتصال به فضای مجازی از طریق تلفن همراه، از ویژگی‌های قابل توجه این

دو فناوری است. با توجه به این مقدمه، پرسش اصلی این است که فناوری اطلاعات به‌ویژه اینترنت و تلفن همراه چه تأثیری بر امنیت ملی جمهوری اسلامی ایران در دهه ۱۳۸۰ داشته است؟ فرضیه موردنظر نیز آن است که هرچند فناوری اطلاعات تهدید جدی برای جمهوری اسلامی ملی ایران در این دهه در بر نداشته ولی با افزایش آسیب‌پذیری کشور، منجر به بروز چالش‌هایی برای امنیت ملی شده است. این چالش‌ها را می‌توان عمدتاً در قالب اختلاف میان دولت و مردم، تهدید ارزش‌های دینی و تضعیف انسجام ملی و افزایش اقدامات بازیگران خارجی علیه نظام مشاهده کرد. این پژوهش درصدد بررسی ارتباط معنادار میان دو متغیر اصلی یعنی فناوری اطلاعات به عنوان متغیر مستقل و امنیت ملی جمهوری اسلامی ایران به عنوان متغیر وابسته است که از روش توصیفی - تبیینی برای فهم و بیان ماهیت این ارتباط استفاده می‌شود. ساختار مقاله نیز به این صورت است که علاوه بر بخش مقدمه و نتیجه‌گیری، دارای سه بخش اصلی است؛ بخش اول با عنوان ادبیات نظری است که به مروری بر مطالعات انجام‌شده، بیان چهارچوب نظری و ارائه تعریفی از متغیرها و ذکر شاخص برای آنها می‌پردازد. در بخش بعدی تأثیر شاخص‌های متغیر مستقل در قالب پارامتر خرد و پارامتر کلان بر شاخص‌های امنیت ملی به عنوان متغیر وابسته بررسی می‌شود و در نهایت بخش سوم با عنوان سنجش فرضیه، به تأثیر فناوری اطلاعات بر امنیت ملی جمهوری اسلامی ایران در قالب پارامتر خرد - کلان می‌پردازد.

### ۱. چهارچوب نظری

در رابطه با تأثیر فناوری اطلاعات بر امنیت ملی ما با دو دسته از مطالعات روبه‌رو هستیم: دسته نخست مطالعاتی هستند که بر تأثیر فناوری اطلاعات بر امنیت ملی از بعد مفهومی و بدون در نظر گرفتن شرایط سیاسی - امنیتی خاص هر کشوری پرداخته‌اند؛ به عبارت دیگر این دسته از منابع عمدتاً به دنبال یافتن نگرش امنیتی بهتر در رابطه با فناوری‌ها هستند. این‌گونه منابع نگاهی تجویزی داشته و غالباً نمی‌توانند به تأثیرات ملموسی که ظهور این فناوری‌ها در بدو ورود به یک جامعه دارند، بپردازند؛ هرچند که چنین منابعی در تدوین سیاست‌های امنیتی با محوریت

امنیت شهروندان و یا امنیت انسانی در تقابل با محوریت دولت و تبدیل تهدیدهای آن به فرصت، سودمند هستند. با توجه به موضوع اصلی این مقاله که به دنبال بررسی تأثیر فناوری اطلاعات بر امنیت ملی کشور با شرایط سیاسی و امنیتی خاص است و همچنین با توجه به آنکه درصدد است این تأثیر را در دهه گذشته بررسی کند، طبیعتاً منابع مذکور که دیدگاهی آینده‌نگرانه دارند پاسخ‌گوی مسئله اصلی مورد نظر نخواهند بود. هرچند باید اذعان داشت در تدوین راهکارها برای مقابله با تهدیدها، این‌گونه منابع بسیار قابل توجه هستند. به عنوان نمونه، مقالاتی که به بررسی تأثیر جهانی شدن بر امنیت ملی ایران پرداخته‌اند (افتخاری، ۱۳۷۹) و همچنین آثاری که در آنها به لزوم بازتعریف انقلاب اسلامی برای تبدیل به بازیگری فعال در عرصه جدید جهانی تأکید شده، در این دسته از مطالعات قرار می‌گیرند (مطهرنیا، ۱۳۸۱).

دسته دوم، مطالعاتی هستند که عمدتاً بر کشور یا کشورهایی مشخص تمرکز داشته و تأثیرات فناوری‌ها را بر امنیت ملی آنها بررسی می‌کنند. این‌گونه مطالعات خود به دو گروه قابل تفکیک‌اند: از یک سو منابعی که به تأثیر فناوری اطلاعات بر امنیت ملی کشورهای توسعه‌یافته با محوریت امریکا پرداخته‌اند. چنین تأثیری عمدتاً به بعد نظامی امنیت ملی و جنگ نامتقارن محدود شده است. به عنوان نمونه جان/اریکسون در کتاب خود با عنوان *روابط بین‌الملل و امنیت در عصر دیجیتال*<sup>(۳)</sup> و در مقاله‌ای با عنوان «فناوری‌های اطلاعات و ارتباطات، راهبرد نامتقارن و امنیت ملی»<sup>(۴)</sup> و همچنین *امیلی گلدمن* در کتاب *امنیت ملی در عصر اطلاعات*<sup>(۵)</sup>، همگی بر کشورهای توسعه‌یافته‌ای تمرکز دارند که به دلیل وابستگی هرچه بیشتر به این فناوری‌ها در مقابل تروریست‌هایی همچون *القاعده* دچار آسیب‌پذیری شده‌اند. آنچه مسلم است آن است که امنیت موردنظر در این دسته از مطالعات به‌طورکامل قابل انطباق با امنیت ملی کشورهای جهان سوم از جمله ایران نیست، زیرا وابستگی زیرساخت‌ها در کشورهای اخیر به گستردگی کشورهای توسعه‌یافته نبوده و نمی‌تواند تهدید جدی‌ای را برای این کشورها در بر داشته باشد. گروه دوم، مطالعاتی هستند که تأثیر فناوری اطلاعات را بر کشورهای جهان سوم بررسی کرده‌اند. در این‌گونه منابع تمرکز اصلی بر ابعاد سیاسی، اجتماعی و فرهنگی امنیت

ملی است که تفاوت آشکاری با مطالعات نظامی محور در گروه اول دارند. آسیب‌پذیری رژیم‌های سیاسی و هویت ملی و تهدیدهای فرهنگی، اقتصادی و اجتماعی از سوی اینترنت مصداق تأثیر فناوری اطلاعات بر امنیت کشورهای جهان سوم است که به عنوان نمونه در آثاری همچون *فناوری اطلاعات و سیاست‌های جهانی* (۵) از مایکل مازار و کتاب *فناوری اطلاعات و سیاست جهانی* (۶) از روزنا و سینگ قابل مشاهده است. قطعاً دیدگاه امنیتی موجود در گروه اخیر به دلیل شباهت بیشتر شرایط سیاسی - امنیتی جمهوری اسلامی ایران با کشورهای جهان سوم، می‌تواند مورد استناد قرار گیرد. در این راستا مطالعات داخلی زیادی صورت گرفته ولی از یک‌سو دیدگاه غالب در این آثار دیدگاه تهدیدمحور و بدبینانه در قالب جنگ نرم است و ضعف دیگر ناشی از نبود چهارچوب نظری مشخص برای تحلیل تأثیر فناوری بر امنیت ملی است. در واقع هرچند بعد از دهمین دوره انتخابات ریاست جمهوری در ایران، مطالب متعددی در رابطه با تأثیر فناوری اطلاعات در حوادث آن نگاشته شد ولی پشتوانه نظری قابل‌قبولی در اکثر آنها وجود نداشته و تنها نوعی بیان توصیفی به کار رفته است؛ بنابراین، پرکردن خلأهای مذکور با نگاهی چندوجهی به تأثیرات فناوری‌های نوین و درعین حال پرداختن به امنیت ملی جمهوری اسلامی ایران به عنوان کشوری در حال توسعه، نوآوری این مقاله به شمار می‌آید.

در دهه‌های پایانی سده بیستم، شاهد موج تازه‌ای از تلاش نظریه‌پردازان برای ارائه چهارچوبی مفهومی در جهت تبیین تحولات موجود در سیاست جهانی بوده‌ایم. علت چنین تلاشی، وقوع تقریباً هرروزه تحولات غیرمترقبه و بلا تکلیفی‌های بسیاری بوده که در همه نقاط جهان وجود دارد و چنان فراگیر و شایع است که ماندگاری شیوه‌های جاافتاده و ریشه‌دار هدایت امور و حفظ امنیت را در معرض تردید قرار می‌دهد. حملات شدید تروریستی مانند حادثه ۱۱ سپتامبر، حمله امریکا به عراق بدون مجوز سازمان ملل، رخنه‌پذیر شدن اقتصادهای ملی در برابر جریان کالا، خدمات و امور مالی، نقض مصونیت سفارتخانه‌ها با توسل به خشونت و موج تازه معارضة‌جویی با اقتدار دولت‌ها در کشورهای مختلف، همگی نوعی خلأ نظری را برای تبیین امور ایجاد کرده‌اند (روزنا، ۱۳۸۴: ۹).

در این میان یکی از تلاش‌های نظری برای فهم تغییرات صورت گرفته، نظریه آشوب<sup>۱</sup> جیمز روزنا است. روزنا سعی داشته از دل هرج و مرج و آشوبی که سیر جاری رویدادها را پدید آورده، به معنایی معقول و قابل فهم دست یابد (روزنا، ۱۳۸۴: ۱۵). برای متمایز ساختن تغییرات آشنا و رایج از دگرگونی‌های عمیقی که امروزه در حال وقوع است باید به ویژگی مهم آشوب یعنی تغییر پارادایم‌ها اشاره کرد؛ زمانی می‌توان قائل به وجود آشوب شد که پارامترهای اساسی سیاست جهانی دستخوش دگرگونی شده و به بروز چالش‌هایی تازه برای امنیت منجر شوند. در شرایط عادی، سه پارامتر سیاست جهان را باثبات نگاه می‌دارد: پارامتر خرد، پارامتر کلان و پارامتر خرد - کلان. پارامتر خرد که روزنا آن را پارامتر مهارت<sup>۲</sup> می‌نامد، به توانایی‌ها و مهارت‌های تحلیلی شهروندان اشاره دارد. در دوره پیشین، مردم با سایر جوامع تماسی نداشته از همین رو نسبت به امور جهان ساده‌انگارانه برخورد می‌کردند. این امر آزادی عمل بسیاری را به رهبران آنها می‌داد، ولی امروزه با افزایش مهارت‌ها، شهروندان می‌توانند در عرصه سیاسی مشارکت بیشتری داشته باشند (طیب، ۱۳۸۰: ۳۴).

منظور از پارامتر کلان یا پارامتر ساختاری<sup>۳</sup>، توزیع قدرتی است که از طریق آن دولت‌ها و سایر نقش‌آفرینان اصلی به یکدیگر واکنش نشان می‌دهند. اگر در گذشته دولت‌ها دارای اقتدار و حاکمیت بوده‌اند، امروزه تغییرات در این پارامتر، منجر به ظهور یک جهان چندمرکزی شده و گروه‌های غیردولتی را به وجود آورده که لزوماً تحت کنترل دولت‌ها نیستند؛ بنابراین، هرچند دولت‌ها هنوز بازیگران اصلی هستند ولی توانایی آنها در مقابل دوگانگی ساختارهای جهانی کاهش یافته است.

پارامتر خرد - کلان که پارامتر مناسباتی<sup>۴</sup> نامیده می‌شود، به مناسبات مرجعیت و اقتدار اشاره دارد که از طریق آنها شهروندان، شرکت‌های چندملیتی، گروه‌های قومی و غیره با جهان دولت‌محوری مرتبط می‌شوند. اگر در گذشته مشروعیت بر

- 
1. Theory of Turbulence
  2. Skill Parameter
  3. Structural Parameter
  4. Relational Parameter

معیارهای سنتی استوار بود، امروزه با گرایش‌های تمرکززدایانه عصر پسا صنعتی، این معیارها به طور روبه‌افزایشی بر مبنای عملکردی قرار دارند که منجر به دشوار شدن اعمال اقتدار به وسیله دولت‌ها می‌شود.

نکته قابل توجه در این نظریه آن است که هرچند روزنا مدل تحلیلی‌اش را بر پایه تک‌علتی قرار نداده و علل متعددی را همچون افزایش شمار بازیگران، جهانی‌شدن اقتصادهای ملی، تضعیف دولت‌ها و تجدید ساختار وفاداری‌ها و گسترش فقر و جهان سوم برمی‌شمارد، ولی در نهایت همه آنها را واکنش به تغییرات چشم‌گیری می‌داند که در فناوری‌های اطلاعاتی رخ داده است. لازم به توضیح است که هریک از سه پارامتر مذکور بیانگر یک سطح تحلیل هستند؛ پارامتر خرد ناظر بر سطح تحلیل امنیت فردی، پارامتر کلان بر امنیت بین‌الملل و پارامتر تلفیق (خرد - کلان) به سطح تحلیل امنیت ملی مربوط است. هرچند روزنا در نظریه خود، تمرکز بیشتری بر پارامتر کلان دارد ولی چون مسئله اصلی ما در اینجا امنیت ملی است، پارامتر تلفیق سطح تحلیل اصلی است که آمیزه‌ای از دو سطح قبل (پارامتر خرد و کلان) است. از آنجایی که دگرگونی در هر پارامتر پیامدهایی برای دیگر پارامترها در بر دارد، در بررسی پارامتر تلفیق ابتدا باید تأثیرات دو پارامتر قبل بر امنیت ملی بررسی شود.

این پژوهش دارای دو متغیر اصلی است: متغیر مستقل که فناوری اطلاعات است و متغیر وابسته یعنی امنیت ملی؛ در ادامه به طور جداگانه تعریفی از هریک از این دو متغیر ارائه می‌گردد.

**فناوری اطلاعات و ارتباطات:** *امانوئل کاستلر* فناوری اطلاعات را «مجموعه همگرای فناوری‌ها در میکروالکترونیک، کاربرد الکترونیک (سخت‌افزار و نرم‌افزار)، مخابرات، رادیو، تلویزیون و الکترونیک نوری» تعریف کرده است (کاستلر، ۱۳۸۰: ۵۹). این فناوری‌ها در دو دسته قرار می‌گیرند: الف) فناوری پردازش اطلاعات (مانند رایانه‌ها، نرم‌افزارها و غیره)؛ ب) فناوری ارتباطات (مانند تلفن، فاکس، ماهواره، کابل‌های نوری و غیره). همان‌طور که پیش از این گفته شد، از میان طیف وسیع فناوری‌های جدید، تمرکز اصلی در اینجا بر روی اینترنت و تلفن همراه است؛ بنابراین، ضرورت دارد که نگاهی به این دو پدیده داشته باشیم.



اینترنت: کلمه اینترنت مخفف شبکه‌های به هم پیوسته<sup>۱</sup> است که منظور از آن شبکه رایانه‌ای است که بنابه تعریف عبارت است از دو یا چند رایانه که از طریق خطوط تلفن، کابل، امواج رادیویی و یا سایر روش‌ها به هم متصل شده‌اند و قادر به مبادله اطلاعات با یکدیگر هستند (قاسم‌زاده، ۱۳۷۹: ۴). به دلیل فاقدِ کانون بودن این پدیده و نامتمرکز بودن آن، پالایش و یا مسدود کردن انواع خاصی از اطلاعات بر روی اینترنت بسیار دشوار است (روزنا و سینگ، ۱۳۹۱: ۲۰۲). ولی آنچه اینترنت را پدیده‌ای انقلابی می‌سازد، تفاوت‌هایی است که نسبت به سایر فناوری‌های پیش از خود دارد: سرعت انتقال اطلاعات، حجم بسیار بالای اطلاعات منتقل شده (سولیمار<sup>۲</sup>، ۱۹۹۹: ۱۸)، سرعت نفوذ و همگانی شدن اینترنت<sup>۳</sup> و در نهایت آنکه تنها پدیده‌ای است که انواع و اشکال گوناگون ارتباطات انسانی و انواع مختلف مضمون و محتوا را به صورت یکپارچه در قالب یک ابررسانه ارائه می‌دهد (میناوندچال، ۱۳۸۱: ۷۲).

تلفن همراه: یکی از مهم‌ترین ویژگی‌هایی که تلفن همراه را از یک پدیده ارتباطی صرف مجزا می‌سازد، امکان اتصال به اینترنت است. بر اساس گزارش‌های موجود، تعداد قابل توجهی از کاربران به‌ویژه در کشورهای توسعه‌یافته، از گوشی خود برای استفاده از اینترنت بهره می‌گیرند. در ایران نیز از سال ۱۳۸۵ با راه‌اندازی شبکه جی‌پی‌آراس<sup>۳</sup> اپراتور دوم تلفن همراه یعنی ایرانسل، برای اولین بار اتصال ۲۴ ساعته به اینترنت از طریق تلفن همراه امکان‌پذیر شد؛ بنابراین، کاربر ایرانی برای اتصال به اینترنت دیگر تنها محدود به رایانه و محیط‌های بسته نبود. با توجه به هزینه اندک این روش نسبت به سایر روش‌های اتصال به اینترنت مانند ADSL، درعین حال سرعت بیشتر آن در مقایسه با اتصال به روش Dial up، در مدت کوتاهی کاربران این نوع از سرویس اینترنتی به میزان قابل توجهی افزایش یافتند تا جایی که اتصال به اینترنت از طریق تلفن همراه در وقایع پس از انتخابات ریاست‌جمهوری در ۱۳۸۸ نقش قابل توجهی ایفا کرد. امکان انجام معاملات مالی، دانلود موزیک و

- 
1. Interconnected Networks
  2. Solymer
  3. GPRS

فیلم، گرفتن عکس و ارسال پیامک نیز از دیگر مزیت‌های این فناوری است. در رابطه با شاخص‌سازی برای متغیر فناوری اطلاعات، لازم به ذکر است که دو پارامتر خرد و کلان به دلیل آنکه تمامی وجوه و شاخص‌های فناوری اطلاعات به‌ویژه شاخص‌های مرتبط با تأثیر آن بر امنیت ملی را نشان می‌دهند، به عنوان شاخص‌های فناوری در نظر گرفته شده‌اند که در بخش مربوطه، توضیح داده می‌شوند.

امنیت ملی: در رابطه با تعریف امنیت ملی اجماع نظر مشخصی وجود ندارد. این امر بیشتر به دلیل عوامل متعددی از جمله عدم تبعیت امنیت از یک تعریف بی‌طرفانه، نارسایی و ابهام سایر مؤلفه‌های وابسته به امنیت (قدرت، منافع، مصالح و غیره)، ماهیت متغیر امنیت (از جامعه‌ای به جامعه دیگر و از زمانی به زمان دیگر) و ذهنی بودن امنیت است (پاتمن<sup>۱</sup>، ۲۰۰۶: ۵۶۹). به همین دلیل، ادبیات امنیت ملی مملو از تعاریف مختلف درباره این مفهوم است ولی غالباً برحسب روابط قدرت میان دولت‌ها و دفاع نظامی در برابر تهدیدهای خارجی مورد بررسی قرار گرفته است؛ ولی امروزه با توجه به پایان جنگ سرد و ظهور عصر اطلاعات چنین تعاریفی تمامی جنبه‌های امنیت ملی را در بر نمی‌گیرد؛ بنابراین، ما نیازمند بازتعریف این مفهوم هستیم.

تعریف پذیرفته‌شده در این پژوهش این است که امنیت ملی، در بُعد عینی، فقدان تهدید نسبت به ارزش‌ها، منافع و اهداف؛ و از نظر ذهنی، فقدان ترس از اینکه این بنیان‌های ملی مورد هجوم (فیزیکی و غیرفیزیکی) واقع بشوند، مورد سنجش قرار می‌دهد. علت انتخاب این تعریف آن است که نخست با ذکر جنبه عینی و ذهنی از امنیت ملی، تهدیدهای نرم را نیز در برمی‌گیرد؛ از سوی دیگر با ذکر واژه بنیان‌های ملی تمامی جنبه‌های نظامی، اقتصادی و اجتماعی را نیز مشمول تعریف کرده و در آخر آنکه، نام نبرد از منبع تهدید نشان‌دهنده آن است که تهدید می‌تواند هم از سوی محیط خارجی و هم محیط داخلی باشد. باتوجه به تعریف ارائه‌شده از امنیت ملی، شاخص‌های این متغیر عبارتند از: منافع ملی و ارزش‌های ملی.

1. Patman

می‌توان گفت ارزش‌ها و هدف‌های اولیه، بنیادین و پایداری را که یک جامعه در صدد تحصیل، حفظ، تثبیت و گسترش آنها در عرصه ملی و بین‌المللی است، منافع ملی می‌گویند (تاجیک، ۱۳۸۱: ۵۳). فارغ از تفاوت میان جوامع، چند شاخص اصلی را می‌توان به عنوان منافع ملی مشترک میان تمامی جوامع تشخیص داد: تمامیت یا یکپارچگی سرزمینی، حفظ نظام سیاسی و ایدئولوژی، هویت و انسجام ملی، رفاه اقتصادی و پیشبرد اهداف ملی. ارزش‌های ملی نیز هنجارها، ایستارها و ارزش‌هایی هستند که پیرامون آنها اجماعی عمومی حاصل آمده و نظام مسلطی را در یک جامعه ایجاد کرده‌اند (تاجیک، ۱۳۸۱: ۹۳). نظام ارزشی در هر جامعه‌ای با نظام تولید اقتدار مرتبط است و در عین حال برای جامعه نظم و انسجام اجتماعی و مشروعیت نهایی به ارمغان می‌آورد. به عنوان نمونه در جامعه ما نظام ارزشی به شدت تحت تأثیر تعالیم دینی قرار دارد (نقیب‌زاده، ۱۳۸۸: ۱۸۲) که تعدیل این نظام ارزشی که تحت تأثیر داده‌های تجدد صورت می‌گیرد، از تهدیدهای اصلی نظام ارزشی ما محسوب می‌شود.

## ۲. تأثیر متغیر فناوری اطلاعات بر امنیت ملی

در این قسمت به منظور بررسی تأثیر اینترنت و تلفن همراه بر امنیت ملی جمهوری اسلامی ایران، ابتدا تأثیر این فناوری‌ها بر پارامتر خرد و پارامتر کلان - به عنوان دو شاخص اصلی برای فناوری اطلاعات - بررسی می‌شود تا پس از آن بتوان در پارامتر تلفیق نتیجه این تأثیرات را بر شاخص‌های امنیت ملی جمهوری اسلامی ارزیابی کرد.

پارامتر خرد، افزایش مهارت افراد: وجوه توانمندی و مهارت افراد در رابطه با امنیت ملی را می‌تواند در چند مورد مشاهده کرد:

الف) بسیج سیاسی همفکران در جهت تحمیل خواسته‌ها: تفاوت این عامل امروز نسبت به گذشته، یکی از بُعد شکل‌گیری ناگهانی اعتراض میان افراد و دیگری از بین بردن مزیت گروه‌های سازماندهی شده نسبت به گروه‌های فاقد نظم از پیش است؛ این مزیت به دلیل آگاهی مشترک<sup>۱</sup> است که به وسیله اینترنت در

اختیار گروه‌های غیرسازماندهی شده قرار می‌گیرد (شیرکی، ۲۰۱۱). به طور مثال جنبش‌های اعتراضی در چهارم فوریه ۲۰۰۸ در کلمبیا هرچند ابتدا به عنوان ایده‌ای در اینترنت و از طریق ابزارهایی چون فیس‌بوک منتشر شد ولی با فراگیری سریع، به بزرگ‌ترین اعتراض‌ها در کلمبیا تبدیل شد (اریکسون، ۲۰۰۹: ۲۰۵).

ب) تولید اطلاعات و دستیابی به منابع متعدد خبری: فضای مجازی نیاز به اتکا به رسانه‌های سنتی یا دولتی برای کسب اطلاعات را از میان برداشته است زیرا افراد می‌توانند به سرعت و سهولت، دیدگاه‌های خود را در آن منتشر کنند. این ویژگی فناوری‌های جدید امکان تبدیل کاربران به تولیدکنندگان محتوا (کاربر - مولف) را فراهم ساخته که این امر نیز چالش‌هایی را برای رسانه‌های سنتی به‌ویژه در کشورهایی که رسانه‌ها رابطه یک‌سویه‌ای را میان دولت و مردم ایجاد می‌کنند، به وجود آورده است (نای، ۱۳۸۹: ۷۵). ماهیت دموکراتیک این فناوری‌ها، امکان شنیده شدن صدای نیروهای حاشیه در جامعه را نیز فراهم می‌کند.

پ) ایجاد و تقویت سپهر عمومی<sup>۲</sup>: این وجه از توانمندی در امتداد همان ایده هابرماس است که ظهور رسانه‌های ارتباطاتی را فرصتی برای ایجاد یک فضای باز منازعه سیاسی و فرهنگی می‌داند که هرگز به‌طور کامل به‌وسیله دولت‌ها اداره و کنترل نمی‌شود (ریتزر<sup>۳</sup>، ۲۰۰۷: ۴۱۹) و تقویت چنین فضایی می‌تواند در دموکراتیک کردن جوامع موثر باشد.

ت) کمک به حفظ و تقویت هویت: افراد مهاجر امکان حفظ هویت خود را در یک سرزمین جدید می‌یابند مانند مهاجران ایتالیایی در فرانسه و یا هویت‌های قومی و اقلیت‌ها که می‌توانند در جهت تقویت و بسیج وجوه هویتی خود برآیند. علاوه بر آن، از آنجایی که اینترنت بستری برای ارائه هویت‌های جدید است، برخی به هویتی فراملی گرایش پیدا می‌کنند (جی.مازار<sup>۴</sup>، ۲۰۰۵: ۵).

ث) توانایی افراد در تولید خشونت: انجام عملیات خرابکارانه بدون نیاز به

- 
1. Shirky
  2. Public Sphere
  3. Ritzer
  4. J.Mazarr

حضور در مکان و سهولت دسترسی به اطلاعات لازم بر روی وب در جهت انجام عملیاتی مانند ساختن سلاح‌های خطرناک، بمب‌های دست‌ساز و غیره امکان این توانمندی را فراهم ساخته است. به عنوان نمونه شبکه بی‌بی‌سی گزارش داد که پیش از بمب‌گذاری ۲۰۰۴ در راه‌آهن مادرید، بمب‌گذاران از دستورالعمل‌های موجود بر روی اینترنت بهره گرفته بودند (روزنا و دیگران، ۱۳۹۰: ۳۵۷).

ابزارهایی که افراد را برای انجام اقدامات مذکور توانمند ساخته‌اند، متعدد هستند که می‌توان مهم‌ترین آنها را وبلاگ‌ها، شبکه‌های اجتماعی مانند فیس‌بوک و توئیتر و امکاناتی که تلفن همراه در اختیار افراد قرار می‌دهد، دانست. علت اهمیت این گونه ابزار نیز خیل عظیم استفاده‌کنندگان، میزان قابل توجه اطلاعاتی که تولید می‌کنند و تأثیرات سیاسی روبه افزایش آنهاست به طوری که امروزه آنها به درون رسانه‌های اصلی وارد شده‌اند و با نقشی که در پیشبرد تحولات اجتماعی و سیاسی ایفا می‌کنند، دیگر نمی‌توان آنها را تنها به عنوان ابزار در نظر گرفت.

**پارامتر کلان، دوگانه‌شدن ساختارهای جهان:** منظور از پارامتر کلان ساختارهای جهانی است که امروزه دستخوش دوگانگی شده‌اند. این دوگانگی ناشی از ظهور بازیگران غیردولتی و بیانگر آن است که دولت‌ها دیگر تنها محل منازعات سیاسی نیستند (ریتزر، ۲۰۰۷: ۴۲۶). امروزه به مدد فناوری‌های نوین، شمار، قدرت و دامنه نفوذ این بازیگران بیشتر شده است. علت آن را باید در ماهیت افقی اطلاعات دانست که به عنوان فراقدرت منجر به فرارفتن مرکزیت اقتدار از محدوده دولت‌ها شده است؛ بنابراین، آنها اقتدار سیاسی متفاوتی را به وجود آورده‌اند که کمتر مبتنی بر سرزمین و بیشتر عملکردی است (کریشنر<sup>۱</sup>، ۲۰۰۶: ۹۳). چند مورد از مهم‌ترین بازیگران جهان چند مرکزی عبارتند از تروریست‌ها که در برخی موارد حضور مؤثری در اینترنت دارند و توانسته‌اند پیروان خود را در جامعه مجازی بیابند و با ابزاری ساده، ویرانی‌های بزرگ خلق کنند؛ سازمان‌های غیردولتی اقتصادی مشروع مانند شرکت‌هایی چون مایکروسافت، اپل و گوگل که منابع مالی آنها از برخی دولت‌ها نیز بیشتر است و یا جرایم سازمان‌یافته‌ای که فناوری اطلاعات امروزه فرصت‌های بسیاری را برای آنها در جهت مشروع‌سازی فعالیت‌ها، افزایش

سود، سازماندهی و ارتباط و محصور نشدن در مرزهای دولتی فراهم کرده است (نای، ۱۳۸۹: ۶۶)؛ نمونه دیگر، سازمان‌های غیرانتفاعی‌اند که هرچند فاقد قدرت اقتصادی و اقتدار قانونی همانند دولت‌ها هستند ولی انقلاب اطلاعات قدرت نرم آنها را بالا برده است (نای، ۲۰۰۲) که منجر به ایجاد شکل جدیدی از حکمرانی بدون حکومت شده است (هالپین و دیگران، ۱۳۸۹: ۱۹۶). یکی از جدیدترین نمونه‌های این نوع بازیگران، ویکی‌لیکس است که به عنوان یک بازیگر آزاد، امکان دستیابی و انتشار هرگونه اطلاعات در فضای مجازی را فارغ از کنترل دولت‌ها ثابت کرده است. در یک جمع‌بندی می‌توان گفت بازیگران غیردولتی امروزه می‌توانند در سطح بالایی نسبت به گذشته فعالیت‌های خود را هماهنگ کنند و با محصور نشدن در مرزهای ملی، به جایی وارد شوند که زمانی حوزه نفوذ امنیت دولت ملی بوده است.

### ۳. سنجش فرضیه در قالب پارامتر خرد - کلان

همان‌گونه که گفته شد این پارامتر پیونددهنده و آمیزه‌ای از دو پارامتر قبل با جهان دولت‌محوری است؛ بنابراین، در اینجا ابتدا باید مشخص شود که تغییرات دو پارامتر پیشین (که در حکم شاخص‌های فناوری اطلاعات بوده‌اند)، چه نتایجی برای امنیت ملی دارد. این نتایج را می‌توان به سه گزاره اصلی تقسیم کرد: اول، تهدید ثبات کشور ناشی از تغییرات پارامتر خرد؛ دوم، تغییر توازن قدرت ناشی از ظهور جهان چندمرکزی و سوم، به چالش کشیده شدن انحصار خشونت ناشی از ظهور حملات سایبری. این سه گزاره تحت‌تأثیر شاخص‌های فناوری اطلاعات بر شاخص‌های امنیت ملی صورت می‌گیرند که در ادامه هرکدام از آنها در رابطه با امنیت ملی جمهوری اسلامی ایران بررسی خواهند شد.

**تهدید ثبات کشور:** این تهدید خود از چند بُعد قابل بررسی است:

الف) تهدید نظام سیاسی و ایدئولوژی: ایدئولوژی سیاسی یک کشور مشروعیت‌دهنده به سیاست‌های حاکمان آن کشور است و در پرتو آن جامعه دارای انسجام و وحدت می‌شود؛ بنابراین، هرگونه تردیدی در ایدئولوژی یک نظام می‌تواند منجر به بی‌ثباتی شود. این درحالی است که فناوری اطلاعات به‌ویژه

اینترنت حفظ ایدئولوژی را بیش از پیش دشوار نموده و این عامل به‌نوعی آسیب‌پذیری برای دولت‌های حاکم تبدیل شده است؛ دلیل آن نیز فرصت‌هایی است که این فناوری‌ها در اختیار افراد گذاشته و مهارت آنها را در جهت زیر ذره‌بین قرار دادن عملکرد دولت‌ها، شک کردن در مشروعیت آنها و بسیج سیاسی در جهت تحمیل خواسته‌ها افزایش داده است (نای، ۲۰۰۲).

ایران تجربه تغییر رژیم و اعتراض‌های سیاسی از طریق ابزارهای ارتباطاتی را در طول تاریخ خود دارد؛ به طور مثال نقش رسانه‌های مطبوعاتی در انقلاب مشروطه و استفاده از نوار کاست‌ها و یا رادیوهای امواج کوتاه در انقلاب اسلامی. بعد از انقلاب و با ورود فناوری‌های نوین به ایران در دهه ۱۳۷۰، فضای مجازی به محیطی برای فعالیت اپوزیسیون تبدیل شد؛ با این توضیح که پیروزی جریان اصلاحات در خرداد ۱۳۷۶ و افزایش انتقاد به نظام سیاسی و مقامات در برخی روزنامه‌ها، منجر به توقیف و بازداشت برخی منتقدان و مخالفان نظام شد (رحیمی، ۲۰۰۳). در واکنش به این توقیف و بازداشت بود که اینترنت به‌ویژه از سال ۱۳۷۸ به عرصه‌ای برای بیان دیدگاه‌های مخالفان داخلی و خارجی تبدیل شد و با حضور بارز در انتخابات ۱۳۸۰، نقش اساسی خود را در حوزه عمومی آغاز کرد و به بخش جدایی‌ناپذیر عرصه سیاسی ایران تبدیل شد. با کنار رفتن جریان اصلاحات از قدرت و روی کار آمدن محمود احمدی‌نژاد در ۱۳۸۴ این‌گونه فعالیت‌ها نیز تشدید شد که اوج آن نیز در حوادث بعد از دهمین دوره انتخابات ریاست‌جمهوری بود. اعتراض‌ها و وقایع بعد از انتخابات که بازتاب وسیعی در تمامی انواع رسانه‌ها داشت، به‌ویژه نقش اینترنت و تلفن همراه را در توانمندی افراد نشان می‌دهد. این توانمندی‌ها حداقل در سه مورد قابل مشاهده است: سازماندهی و هماهنگی فعالیت‌ها، انتشار اخبار و وقایع مربوط به حوادث ایران، بسیج ایرانیان خارج از کشور.

سازماندهی و هماهنگی فعالیت‌ها: کمتر کسی است که در رابطه با نقش بارز فضای مجازی در سازماندهی فعالیت‌ها تردید داشته باشد. راه‌اندازی تجمعات و اعلام روز و ساعت دقیق آن، بهره‌گیری از نمادهای هماهنگ مانند رنگ سبز و

شعارهای مشخص آن هم در مدت زمان کوتاه و در حد وسیع، تنها با استفاده از ابزارهایی چون شبکه‌های اجتماعی ممکن شده بود. وجود صفحات، پست وال<sup>۱</sup> و فیدهای<sup>۲</sup> متعدد با موضوع انتخابات ایران و شمار بسیار اعضای آنها، دلالت بر نقش وسیع شبکه‌هایی چون فیس‌بوک و توییتر در این حوادث داشت.

انتشار اخبار و وقایع مربوط به حوادث ایران: درحالی که رسانه‌های داخلی از پوشش دادن اخبار و وقایع بعد از انتخابات منع شده بودند، انتشار اخبار برای معترضان از طریق وبلاگ‌ها و شبکه‌های اجتماعی ممکن شده بود، به طوری که حتی خبرگزاری‌های رسمی خارجی نیز بسیاری از اخبار خود را از این منابع می‌گرفتند. هرچند این اخبار و اطلاعات بسیار ضدونقیض و بی‌نظم و منشأ تولید شایعه و پراکندن دروغ بود؛ با وجود این از آنجایی که بر خلاف خواست دولت و با وجود منع رسمی از سوی آن اتفاق می‌افتاد، چالشی امنیتی محسوب می‌شد.

بسیج ایرانیان خارج از کشور: یکی از مهم‌ترین نتایج تبدیل فضای مجازی به رسانه‌ای برای اعتراض‌ها و درگیری‌ها در ایران، توجه ایرانیان مخالف نظام در خارج از کشور به وقایع داخلی ایران و بسیج آنها در جهت حمایت از معترضان داخلی بود. تجمعات اعتراض‌آمیز در مقابل سازمان ملل در نیویورک، اطراف برج ایفل در پاریس، مقابل سفارت ایران در ایتالیا و امارات، همگی نشان‌دهنده گستردگی بسیج مخالفان بوده که پای کشورهای غربی به‌ویژه آمریکا و انگلیس را نیز با وجود ادعای بی‌طرفی اولیه، به حوادث باز کرد.

به عنوان یک نتیجه‌گیری می‌توان گفت حوادث بعد از انتخابات که افزایش توانمندی افراد در مقابل دولت را نشان می‌دهد به چالشی برای امنیت ملی تبدیل شد. این چالش به‌ویژه از سوی اختلاف میان دولت و مردم و کاهش مشروعیت دولت از دیدگاه معترضان بوده که به عقیده باری بوزان چنین تنش می‌تواند منشأ بزرگ‌ترین ضعف و آسیب‌پذیری باشد (بوزان، ۱۳۷۸: ۹۹). این چالش امنیتی پس از فروکش کردن حوادث انتخابات نیز تا حدودی باقی ماند. قرارهای دسته‌جمعی که برخی افراد از طریق شبکه‌هایی مانند فیس‌بوک می‌گذاشتند هرچند شکل سیاسی

1. Post wall  
2. Feeds



نداشت ولی نگرش امنیتی دولت به آنها، نشان از وجود آسیب‌پذیری دولت از این بُعد دارد.

ب) تهدید هویت ملی و تمامیت سرزمینی: هویت ملی یک احساس جمعی مشترک است که منجر به ایجاد همبستگی میان افراد در چهارچوب سرزمینی مشخص می‌شود؛ بنابراین، خلق و تداوم چنین هویتی از سوی دولت حائز اهمیت بسیار است (رحمت‌اللهی، ۱۳۸۴: ۹۲). این درحالی است که ظهور فناوری‌های نوین، توانایی دولت‌ها را در این زمینه کاهش داده است. در رابطه با ایران این تهدید از دو بُعد قابل بررسی است: اول آنکه ارزش‌های جهانی شدن که به عنوان ارزش مسلط در این فناوری‌ها قرار دارد، به دنبال قلع و قمع هویت ملی - اسلامی است. نظرسنجی‌های صورت‌گرفته در این زمینه به‌ویژه در میان قشر جوان نیز دلالت بر تضعیف هویت ملی دارد.<sup>(۸)</sup> تهدید دیگر از بُعد 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 تا در جهت بسیج سیاسی هرچه بیشتر حرکت کنند مانند جامعه کردهای امریکا<sup>۱</sup> که در فضای مجازی ایجاد شده از طریق وب‌سایت خود<sup>(۹)</sup> به تسهیل دستیابی به اهداف ملت کرد کمک می‌کند (جی. مازار، ۲۰۰۵: ۲۰). توانمند شدن این گروه‌ها و تشدید فعالیت آنها، علاوه بر تضعیف انسجام ملی می‌تواند تمامیت سرزمینی را نیز با تهدید روبه‌رو سازد.

پ) تهدید ارزش‌های ملی: از آنجایی که مهم‌ترین کارویژه ارزش‌های ملی حفظ همبستگی و مشروعیت‌دهنده به قواعد و ضوابط اجتماعی است، هرگونه تهدید معطوف به آنها می‌تواند بی‌ثبات‌کننده نظام سیاسی یک کشور باشد. تهدید فرهنگ و ارزش‌های جامعه ایران، باید از دو بُعد مورد بررسی قرار گیرد: یکی تهدید ارزش‌ها به صورت یک برنامه از پیش تعیین شده و غیرخسونت‌آمیز به‌منظور تغییر نظام سیاسی کشور (ای. پرایس<sup>۲</sup>، ۲۰۰۲: ۵۵) که امروزه ظهور اینترنت شدت و دامنه این‌گونه فعالیت‌ها را وسیع‌تر ساخته است. این تهدیدها که در قالب جنگ نرم صورت

1. American Kurdish Association  
2. E.Price

گرفته و با تهدیدهای سابق یعنی نظامی و اقتصادی ماهیت متفاوتی دارد و در راستای دیدگاه ابزارگرایانه<sup>(۱۰)</sup> دولت‌های غربی به فناوری‌های نوین (دامبرل<sup>۱</sup>، ۲۰۰۷) قرار دارد. 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 یک فضای چندارزشی تبدیل کرده است (تاجیک، ۱۳۸۱: ۱۶۵). همان‌گونه که آلون 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 کرده‌است این درحالی است که 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. تغییر توازن قدرت: علاوه بر تهدید ثبات یک کشور، تأثیر دیگر فناوری اطلاعات بر امنیت ملی کشورها، تغییر توازن قدرت است که در نتیجه توانمند شدن بازیگران غیردولتی رخ می‌دهد. انقلاب اطلاعات بر توان و قدرت 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 (ریتزر، ۲۰۰۵: ۴۰۳). در رابطه با امنیت ملی جمهوری اسلامی می‌توان به چهار بازیگر غیردولتی اشاره داشت که هر چند تا کنون تهدید جدی علیه حاکمیت دولت ایجاد نکرده‌اند ولی فناوری‌های نوین با تقویت این گروه‌ها، می‌توانند چالش‌هایی را برای امنیت ملی به وجود آورند:

الف) سازمان‌های مدافع حقوق بشر: واقعیتی که در رابطه با نهادهای حقوق بشر - به‌رغم افزایش توانایی آنها در محیط بین‌الملل - نباید نادیده گرفت، آن است که هر چند این‌گونه سازمان‌ها به صدور گزارش‌ها و بیانیه‌های متعددی علیه نقض حقوق بشر در ایران پرداخته‌اند ولی تأثیر جدی در رابطه با امنیت ملی و رویه‌ها و تصمیم‌گیری‌های داخلی و خارجی نداشته‌اند؛ هر چند ممکن است دولت تحت فشار رسانه‌ها ناگزیر از واکنش نشان دادن شود ولی آنها به‌ندرت توانسته‌اند مانع یک تصمیم یا تغییر موضع شوند (صالحی، انتخابی، سلطانی‌فر، ۱۳۸۷: ۳۳). با

وجود این، یکی از پیامدهای گزارش این نهادها علیه نظام، تأمین محتوا برای مخالفان است. از آنجایی که مخالفان نظام، این نهادها را بازیگرانی مشروع و قانونی می‌دانند، اخبار و مطالب آنها می‌تواند دستاویز بیشتری را برای مخالفان در جهت اهداف خود فراهم سازد. از دیگر پیامدهای منفی ناشی از فعالیت این بازیگران، مخدوش‌سازی اعتبار و چهره ایران در برابر افکار عمومی جهان است. علاوه بر آن نمی‌توان این امر را نادیده گرفت که این سازمان‌ها با استفاده از قدرت و سرمایه کشورهای غربی و با تحمیل فرهنگ و ارزش‌های این کشورها در قالب قوانین حقوق بشر، می‌توانند به حذف بسیاری از فرهنگ‌ها، هویت‌های ملی و محلی بپردازند. درحالی‌که سازمان‌های مردم‌نهاد در اصل، وظیفه حمایت و حراست از این هویت‌ها را بر عهده دارند (رحمت‌اللهی، ۱۳۸۴: ۹۵).

ب) جنبش زنان: تلاش برای اسلامی کردن جامعه ایران بعد از انقلاب اسلامی، مباحث بسیاری را ایجاد کرد. افزایش شهرنشینی، افزایش سطح سواد و دستیابی به آموزش و درعین حال وجود برخی ملاحظات در سیاست‌های دولت، منجر به 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 رابطه با زنان را به چالش کشیدند. تحت تأثیر فعالیت زنان، برخی بر این باورند که وبلاگ‌ها مکانی را ایجاد نموده‌اند که در آن ارزش‌های جمهوری اسلامی در رابطه با زنان و خانواده به چالش کشیده می‌شود، به همین دلیل افزایش این نوع فعالیت‌ها نگران‌کننده است. به عنوان نمونه آنها در مخالفت با بسیاری از قوانین همچون سنگسار و یا ازدواج موقت، اعتراض‌های خود را در فضای مجازی دنبال کرده‌اند و گروه‌هایی همچون کمپین یک میلیون امضا که درصدد تغییر برخی قوانین هستند که تصور می‌شود تبعیض‌آمیز است، فعالیت خود را عمدتاً از طریق اینترنت به پیش می‌برند. به‌طور کلی نتیجه ظهور فضای مجازی در رابطه با قشر زنان، افزایش حضور آنها در این فضا به عنوان نوعی جبران از کمبود حضور آنها در دنیای واقعی در مقابل مردان است؛ علاوه بر آن حضور چنین جنبش‌هایی می‌تواند تهدیدی برای ارزش‌های اسلامی جامعه محسوب شود.

پ) جنبش چپ‌ها: یکی دیگر از فعالیت‌های قابل توجه در اینترنت، فعالیت

گروه‌هایی با گرایش‌های چپ است. بسیاری از سایت‌ها و وبلاگ‌ها درصد متحد ساختن این گروه‌ها برای اعتراض‌ها و بیان دیدگاه‌های خود و این نکته هستند چطور اتحادیه‌ها و گروه‌های مختلف اهداف و اقدامات خود را هماهنگ سازند، ولی آنچه در فعالیت آنها بارز است آن است که بیشتر اعضای آنها نه کارگران بلکه دانشجویان رادیکال چپ هستند. فعالیت دانشجویان چپ قبل از پیروزی انقلاب اسلامی در دانشگاه‌ها قابل توجه بود ولی این حرکت‌ها بعد از انقلاب اسلامی به دلیل عدم دستیابی به اهداف خود کم‌رنگ‌تر شد و به‌رغم حضور گسترده بر روی وب تا کنون به غیر از برخی اعتراض‌های دانشجویی و یا اعتصاب‌های کارگری، تهدیدی برای امنیت جمهوری اسلامی در پی نداشته‌اند.

ت) ایرانیان خارج از کشور: مهاجرت از ایران با وقوع انقلاب اسلامی افزایش یافت. اهمیت این موضوع از این جهت است که این جمعیت به‌خوبی در اینترنت حضور دارند و بخشی از آنها از فضای مجازی علیه جمهوری اسلامی ایران بهره می‌گیرند، در نتیجه ارتباط آنها با ایرانیان و تعداد مخاطبان آنها در داخل افزایش یافته است. عباس میلانی یکی از سرپرستان پروژه دموکراسی/ایران در مؤسسه هور امریکا 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. در بررسی که دو محقق خارجی<sup>۱</sup> در زمینه وبلاگ‌های فارسی انجام داده‌اند، دریافته‌اند که از میان چهار گروه محتوای وبلاگ (سکولار/اصلاح طلب، شعر و ادبیات، مذهبی/محافظه‌کار و گروه چهارم آمیزه‌ای از موضوعات مختلف)، بیشترین تعداد مربوط به وبلاگ‌های سکولار بودند که بیشتر آنها نیز در خارج از ایران قرار داشتند (نفیسی<sup>۲</sup>، ۲۰۰۸: ۱۷-۱۴). تشویق ایرانیان در داخل به ایجاد اعتراض علیه دولت یکی از مهم‌ترین اهداف حضور آنها در فضای مجازی است.

در یک جمع‌بندی از نقش بازیگران غیردولتی در ایران می‌توان دو نتیجه اصلی گرفت: نخست آنکه تأثیر این سازمان‌ها در ایران چندان وسیع و قابل توجه نیست؛

1. Kelly and Etling  
2. Nafisi

شاید یکی از علل آن ناشی از تقابل این جمعیت‌ها به عنوان سازمان‌هایی مدرن با سازمان‌هایی است که مبتنی بر اجتماعات سنتی در ایران هستند؛ جوامعی که اساساً بر فعالیت‌های مذهبی و عقیدتی تمرکز دارند. دیگر آنکه، به‌رغم اندک بودن، توسعه‌نیافتگی و عدم تأثیرگذاری جدی این بازیگران، فضای مجازی به مکانی برای بیان اعتراض‌هایی تبدیل شده که در فضای عمومی جامعه قابل طرح نیست. این عامل در بلندمدت می‌تواند چالش‌هایی برای سیاست‌های دولت و آینده نظام سیاسی پدید آورد.

**حملات سایبری و 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، منجر به 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 و یا خشونت نمادین استفاده شود (نای، ۲۰۱۱: ۴۵). موضوعیت یافتن این نوع از 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 (آلبرتس و پاپ، ۱۹۹۷: ۱۴۷). گفتنی است که حملات سایبری تنها در تقابل میان جهان دولت‌محور با افراد و بازیگران غیردولتی اتفاق نمی‌افتد بلکه این نوع از جنگ (جنگ نامتقارن) توزیع قدرت میان دولت‌ها را نیز تغییر داده است. در این میان قدرت غالباً به سود آنهایی که زمانی بازیگران کوچک‌تر انگاشته می‌شدند، بازتوزیع می‌شود (طیب، ۱۳۸۹: ۲۸۰).

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 ضربه‌زدن به فعالیت‌های هسته‌ای ایران بخش یا بخش‌هایی از زیرساخت‌های صنعتی کشور را آلوده ساخته‌اند، از این دست بوده‌اند. ولی می‌توان گفت مهم‌ترین حمله جدی از این نوع در دهه ۸۰، ویروس استاکس‌نت<sup>۲</sup> بوده است.

1. Alberts & Papp  
2. Stuxnet

این کرم رایانه‌ای یک حمله تروریستی سایبری محسوب می‌شد که نخستین بار در ماه ژوئن ۲۰۱۰ شناسایی شد. از آنجایی که هدف اصلی این حملات فعالیت‌های هسته‌ای ایران بود و با توجه به حجم بالای طراحی و دانش تخصصی به‌کاررفته 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). زیرا برخی از تحلیل‌گران و افسران سابق ارتش امریکا حملات سایبری به تأسیسات هسته‌ای ایران را مؤثرتر از بمباران آنها می‌پنداشتند. البته از آنجایی که دولت‌ها به دلیل سلب اعتماد از توانایی‌هایشان تمایلی به گزارش چنین حملاتی ندارند، نمی‌توان به‌طور دقیق تأثیرات استاکس‌نت را ارزیابی کرد. به عنوان نمونه برخی از مقامات ایرانی از جمله *علی اصغر سلطانیه*، نماینده ایران در آژانس بین‌المللی انرژی اتمی، تأکید داشت که ویروس استاکس‌نت تأثیری بر فعالیت‌های هسته‌ای جمهوری اسلامی نداشته است. *غلامرضا جلالی* رئیس سازمان پدافند غیرعامل ایران نیز ویروس استاکس‌نت را حامل مشکلاتی برای کشور می‌دانست ولی در عین حال قائل به کنترل و خنثی شدن آن در بخش‌های عمده‌ای بود.<sup>(۱)</sup> علاوه بر آن در مقاله‌ای که در مؤسسه خاور نزدیک و واشنگتن به بررسی تأثیر ویروس استاکس‌نت بر تأسیسات هسته‌ای ایران و از کار انداختن سانتریفیوژها پرداخته، تأکید شده که این ویروس در نابودی همه سانتریفیوژها در نیروگاه نطنز به هدف خود نرسیده، ولی منجر به نابودی تعداد محدودتری از سانتریفیوژها و به تأخیر انداختن موقت پیشرفت ایران در نطنز، موفق بوده است (آلبرایت، ۲۰۱۰).

با وجود این برخی متخصصان امنیتی در این حوزه معتقدند که این ویروس بزرگ‌ترین و سازمان‌یافته‌ترین حمله سایبری تاریخ را رقم زد و کد استاکس‌نت، طولانی‌ترین کدی بوده 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 ناگازاکی آوردند؛ آن‌هم تنها با تکثیر

1. Albright

قارچ‌گونه از طریق فلش‌های یواس‌بی.<sup>(۱۳)</sup>

برخی دیگر از حملات سایبری، از بعد سیاست نمادین و حقارت ملی قابل تفسیر است مانند هک کردن و از دسترس خارج ساختن سایت‌ها که هرچند خصومت کمتری دارد ولی نشان‌دهنده تحقیر، توهین و جریحه‌دار ساختن غرور ملی است (روزنا و دیگران، ۱۳۹۰: ۳۱). این نوع از جنگ را بیشتر تفاسیر سازه‌انگاران از انقلاب اطلاعات مورد توجه قرار داده‌اند. آن دسته از بازی‌های رایانه‌ای که عمدتاً از سوی نیروهای نظامی طراحی شده و دارای پیام‌های سیاسی هستند نیز در این راستا قرار می‌گیرند. امروزه تروریسم موضوع جذابی برای بسیاری از بازی‌های رایانه‌ای است که نمادها و تصاویری از مسلمانان را مورد حمله قرار می‌دهند.

یکی از مهم‌ترین آسیب‌پذیری‌های ایران در رابطه با حملات سایبری، در رابطه با ضعف زیرساخت‌هاست. به طور نمونه هرچه تعداد کاربران و فعالیت‌های اینترنتی افزایش می‌یابد تقاضا برای پهنای باند<sup>(۱۴)</sup> به‌منظور از عهده برآمدن ارتباطات روبه‌رشد اینترنتی نیز بیشتر می‌شود؛ این درحالی است که به دلیل مقرون‌به‌صرفه بودن ارتباطات اینترنتی از طریق ماهواره‌ها، بیشتر کشورهای درحال توسعه این راه را انتخاب می‌کنند. بهره‌گیری از این روش به دلیل آنکه باعث می‌شود همه اطلاعات از یک نقطه مرکزی انتقال یابد و همچنین از کارانداختن ماهواره‌ها به وسیله جنگ‌افزارهای لیزری و یا پارازیت انداختن بر روی آنها، از جمله مهم‌ترین آسیب‌پذیری است که می‌تواند آماجی برای سوءاستفاده دشمنان بالقوه باشد (هالپین و دیگران، ۱۳۸۹: ۲۲۵). اتکای بیش از حد صنعت اطلاعات به تجهیزات خارجی، نارسایی و ناکافی بودن تأسیسات امنیتی، ناتوانی برای سنجش ایمنی تجهیزات وارداتی و عدم آگاهی جامعه از اهمیت ایمنی اطلاعات، دیگر تهدیدهایی است که امنیت را در جامعه به خطر می‌اندازد (هالپین و دیگران، ۱۳۸۹: ۳۳۲)؛ بنابراین، می‌توان گفت هرچند تا کنون حملات سایبری برای امنیت ملی جمهوری اسلامی ایران در قالب تهدیدی جدی مطرح نبوده ولی در صورت نبود راهکار جدی برای تأمین امنیت شبکه، تضمینی برای عدم وقوع چنین تهدیدهایی در آینده وجود نخواهد داشت.

## نتیجه‌گیری

هرچند فناوری اطلاعات تأثیرات مثبتی همچون افزایش ارتباط میان دولت‌ها و افراد، بهبود روابط دیپلماتیک، توانمند شدن افراد در جهت مشارکت هرچه بیشتر در سیاست‌های داخلی و خارجی و غیره دارد ولی این تمام داستان نیست زیرا این فناوری‌ها به‌ویژه برای آن دسته از کشورهایی که تنها واردکننده آنها بوده‌اند، تهدیدهایی نیز به همراه داشته است. یکی از نمونه‌های این جوامع جمهوری اسلامی ایران است که این پژوهش اساساً واکنشی است به مواجهه اجتناب‌ناپذیر یک جامعه سیاسی با موج جدیدی از فناوری که تقریباً نقشی در ایجاد آن نداشته است.

از مطالعات انجام‌شده می‌توان نتیجه گرفت که فناوری اطلاعات در دهه ۱۳۸۰ تهدید جدی‌ای را متوجه امنیت ملی نساخته؛ با این حال آسیب‌پذیری کشور را در برخی مؤلفه‌های آن برجسته کرده است. این آسیب‌پذیری عمدتاً از دو بعد بوده است: اول، توانمند شدن شهروندان که به‌ویژه در برخی مقاطع زمانی منجر به سمت‌گیری برخی از افراد در تقابل با دولت شد؛ دوم، آسیب‌پذیری از سوی اقدامات بازیگران خارجی که فضای مجازی در سال‌های اخیر شدت این‌گونه فعالیت‌ها را بیش‌ازپیش ساخته است. این درحالی است که دیپلماسی قوی و مؤثری نیز از سوی ایران در جهت مقابله با این اقدامات صورت نگرفته است. علاوه بر این دو مورد، چالش امنیتی دیگر، تهدید ارزش‌های ملی و تضعیف انسجام ملی است. این چالش به دلیل ارزش‌های لیبرالی است که در تضاد با ارزش‌های دینی و بعد دینی هویت نظام سیاسی است.

ولی پیش از آنکه برخی راهکارها در مواجهه با تهدیدهای ناشی از این فناوری‌ها ارائه شود، ابتدا اقدامات انجام‌شده به‌وسیله دولت در دهه ۱۳۸۰ در برابر تهدیدهای مذکور بررسی می‌شود تا نقاط قوت و ضعف دولت در این راستا مشخص شده و بتوان به صورت واقع‌بینانه به ارائه راهکارها پرداخت. در رابطه با واکنش دولت در برابر تهدیدها، می‌توان چهار اقدام اصلی را مشاهده کرد:

۱. مانیتورینگ و ردیابی مخالفان: فضای مجازی؛ ردیابی مخالفان، شناسایی و مجازات آنها را از سوی دولت آسان کرده است. در حوادث پس از انتخابات دهمین



دوره ریاست جمهوری، شبکه‌های اجتماعی به دولت امکان نظارت و ردیابی معترضان را می‌دادند (گراسمن<sup>۱</sup>، ۲۰۰۹). به این ترتیب دولت در دادگاه‌هایی که علیه مجرمان بعد از انتخابات برگزار کرد، توانست ثابت کند که برخی از مخالفان در داخل چگونه و با چه افرادی در خارج ارتباط دارند. مورد دیگر نیز امکان شنود مکالمات و ردیابی افراد از طریق تجهیزات مانیتورینگ تلفن همراه است.<sup>(۱۴)</sup>

۲. کنترل فعالیت‌های آنلاین و فیلترینگ فضای مجازی: می‌توان گفت تا سال ۱۳۸۲ دولت استراتژی نظام‌مندی برای مسدود کردن و یا فیلتر کردن محتوای اینترنت صورت نداد (رحیمی، ۲۰۰۳) ولی با افزایش فعالیت‌ها بر روی وب و افزایش تعداد کاربران، از سال ۱۳۸۰ محدودیت‌هایی رسمی بر استفاده از اینترنت اعمال شد. این محدودیت‌ها بیشتر متوجه سایت‌هایی با محتوای ضد اسلامی، غیراخلاقی و مطالبی بود که از لحاظ سیاسی تهدید امنیت ملی محسوب می‌شدند. تشکیل کمیته تعیین مصادیق فیلترینگ نیز در همین راستا قرار دارد. در جریان وقایع پس از انتخابات، علاوه بر فیلتر شدن برخی شبکه‌های اجتماعی، از تاریخ ۲۲ خرداد ۱۳۸۸ خدمات پیام کوتاه نیز مختل شد و با تداوم قطعی شانزده‌روزه این سیستم، ایران رکورد بالاترین مدت زمان قطعی پیامک در جهان را از آن خود کرد (ضیایی‌پرور، ۱۳۹۰).

۳. تبلیغات سیاسی در وب به نفع دولت: از همان ابتدای ورود اینترنت به ایران، دولت نیز به بهره‌گیری از فضای مجازی در جهت تحقق اهداف و ترویج دیدگاه‌های خود پرداخت و این نشان‌دهنده آن است که حتی سنت‌گرایان نیز نمی‌توانند نسبت به آن بی‌تفاوت باشند؛ به عنوان مثال محمدحسین صفارهرندی وزیر سابق وزارت فرهنگ و ارشاد اسلامی اعلام کرده بود عنوان معاونت مطبوعاتی باید به معاونت رسانه‌ای تغییر یابد تا بتواند شامل اینترنت و وبلاگ نیز شود (مینا<sup>۲</sup>، ۲۰۰۷). استفاده روحانیت به‌ویژه حوزه علمیه قم از فضای مجازی نیز در همین راستا قابل بررسی است. به‌طوری‌که اکنون بسیاری از مراجع تقلید نیز دارای وبسایت اختصاصی هستند.

1. Grossman  
2. Mina

۴. حملات سایبری: همان‌گونه که ایران تا کنون مورد تهدید جدی حملات سایبری به غیر از ویروس استاکس‌نت قرار نگرفته، حملات سایبری گسترده‌ای را نیز صورت نداده است. حملات سایبری اساساً در قالب هک کردن سایت مخالفان است. به عنوان نمونه سایت گرداب در چند نوبت توانست برخی سایت‌ها همچون سایت رسمی سازمان ملل، سایت اصلی دولت اسرائیل<sup>(۱۵)</sup>، سایت آپیاک<sup>۱</sup> (لابی اسرائیل در امریکا) را از دسترس خارج سازد. همچنین حمله به وبسایت انتشاردهنده کاریکاتورهای موهن پیامبر (ص) به وسیله گروه امنیتی آشیانه و حمله به ۴۸ وبلاگ مبتدل و توهین‌کننده روی سرویس‌دهنده بلاگفا به وسیله گروه جهاد مجازی نیز از دیگر اقدامات در عرصه حملات سایبری است.

به عنوان یک نتیجه‌گیری می‌توان گفت دولت در بخش اقدامات تدافعی، فعال‌تر عمل کرده است، به طوری که هرچند در رابطه با گزینه تبلیغ در فضای مجازی به نفع نظام سیاسی - که در قالب دیپلماسی عمومی تعریف می‌شود - اقداماتی را صورت داده ولی در این زمینه چندان قوی نبوده و نتوانسته مخاطبان وسیعی را جذب کند. به طور مثال در جریان فعالیت‌های هسته‌ای و اثبات صلح‌آمیز بودن آن نزد افکار عمومی در دهه ۸۰ دولت نتوانست اقدامی جدی صورت دهد؛ در مقابل تبلیغات رسانه‌های غربی و تأثیرگذاری آنها بر مردم عادی و روزنامه‌نگاران منجر به آن شد تا بیشتر افکار عمومی جهان متقاعد شوند ایران فعالیت‌های خود را از آژانس مخفی می‌کند. از سوی دیگر برخوردهای مقطعی و انفعالی می‌تواند نتیجه معکوسی در پی داشته باشد زیرا نگرش سیاسی و امنیتی به فضای مجازی و محدود ساختن دسترسی به آن ممکن است در نبود فضایی برای طرح دیدگاه‌های مخالف، منجر به تمایل بیشتر افراد به‌ویژه قشر جوان جامعه به محتوا و ارزش‌های موجود در این فناوری‌ها و همچنین سیاسی‌شدن قشر غیرسیاسی و رادیکال‌تر شدن کنشگر سیاسی شود؛ بنابراین، غفلت از این فناوری‌ها که منشأ پیشرفت در بسیاری از کشورها شده‌اند، در آینده‌ای نه‌چندان دور کشور را دچار تحیر و سرگردانی خواهد کرد؛ به همین دلیل، ارائه راهکارهایی برای مقابله اصولی‌تر با تهدیدهای ناشی از آنها ضروری می‌نماید.

1. AIPAC

## ارائه راهکار

پیش از تدوین راهکارها، باید به این نکته توجه داشت که هرچند تهدیدهای گفته‌شده، ناشی از فناوری اطلاعات است ولی راه‌حل‌های مقابله با آنها را نمی‌توان تنها به حوزه این فناوری‌ها محدود کرد بلکه نیازمند اقدام در حوزه‌های غیرفناورانه همچون اقتصاد، جامعه و فرهنگ نیز هست (جین، ۱۳۸۵: ۴۸-۵۶). با توجه به این نکته، در ادامه برخی راهکارها ارائه می‌گردد:

۱. تقویت بخش خصوصی: باید پذیرفت که تنها راه توسعه فناوری اطلاعات، از مسیر تقویت بخش خصوصی می‌گذرد. البته خصوصی‌سازی به معنای توسعه این صنعت صرفاً بر اساس 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 و به سیاست‌گذاری و نظارت پردازد.

۲. توسعه اقتصادی: فناوری اطلاعات با کاهش هزینه‌ها، افزایش کیفیت و ایجاد ارزش افزوده، فرصت‌های بسیاری را برای توسعه اقتصادی ایجاد می‌کند (روزنا و سینگ، ۱۳۹۱: ۳۸۹). به عنوان 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 خطرات به گونه‌ای ملایم و ناملموس حراست می‌کند (پورسعید، ۱۳۸۸). یکی از رموز وقوع انقلاب اسلامی نیز انتشار پیام نرم صلح و عدالت در بیرون از مرزهای خود بود؛ بنابراین، در سده ۲۱ نیز قدرت نرم و پیام نرم باید رویکرد محوری نظام باشد. به این ترتیب برخورد با تهدیدهای محتوایی در اینترنت باید به صورت مهار غیرمستقیم بوده و از طریق سازوکارهای اجتماعی از جمله نهادینه کردن اخلاق عمومی صورت گیرد. بُعد دیگر امنیت نرم، رویکرد ایجابی به امنیت ملی است. در این رویکرد جدید به امنیت، به جای «امنیت برای حکومت‌ها»، صحبت از «امنیت

برای مردم» است؛ یعنی وضعیتی که در آن میان خواسته‌های ملی و کارآمدی نظام سیاسی نسبت متعادلی وجود داشته باشد به‌گونه‌ای که در شهروندان تولید رضایت کند (احمدیان، ۱۳۸۰). این رویکرد نقطه مقابل رویکرد سلبی و دولت محور به امنیت ملی است که در آن نگرانی پیوسته در رابطه با تهدیدهای بیرونی است تا آسیب‌های درونی و نگرانی‌ای در رابطه با نوع سیاست و رفتار حاکمان در داخل وجود ندارد (نای، ۱۳۸۹: ۱۸).

۴. ایجاد توازن در ابعاد هویتی: این راهکار در واقع در جهت حفظ و تقویت انسجام ملی است. هرچند ایران کشوری قومیتی است، با این وجود اقلیت‌های ساکن در ایران اساساً ایرانی هستند به این ترتیب در برخورد با آنها نباید به دید اقلیت رفتار شود (نقیب‌زاده، ۱۳۸۸: ۱۹۷). سازنده‌ترین راه، شریک کردن گروه‌های قومی در قدرت است. نکته دیگر تقویت هویت ملی از طریق توازن در ابعاد دینی و ملی هویت است؛ در رژیم گذشته به ارزش‌های دینی بی‌اعتنایی می‌شد و اکنون باید تلاش بر این باشد تا ارزش‌های ملی مورد کم‌توجهی قرار نگیرد. این درحالی است که عدم تأکید بر پیوند میان آنها، ممکن است منجر به بروز چالش‌هایی برای نظام سیاسی شود زیرا در عصر اطلاعات، افراد بیشتر مستعد پذیرش فرهنگ‌ها و الگوهای بیگانه هستند.

۵. تقویت دیپلماسی عمومی: فراوانی اطلاعات در عصر کنونی منجر به فقر توجه و تمرکز بر اطلاعاتی خاص می‌شود، همین عامل منبع قدرتی را برای آنها می‌تواند به ما بگویند توجه‌مان را کجا متمرکز سازیم، ایجاد می‌کند (نای، ۲۰۱۱). ایران نیز باید خود را به نوع نوین دیپلماسی نفوذ برای تأثیرگذاری یا تغییر فضای رسانه‌ای خارج از مرزها مجهز سازد. این اقدام در گروه اقدامات فعالانه و نقطه مقابل اقدامات منفعلانه‌ای است که وجه غالب اقدامات در مقابل تهدیدها است. البته دیپلماسی رسانه‌ای هنگامی تأثیر واقعی خود را می‌گذارد که به وسیله غیردولتی‌ها اعمال شود.

۶. انعطاف‌پذیری فرهنگی: هرچند امروزه عناصر فرهنگ غربی به وسیله فناوری اطلاعات وارد فرهنگ ایرانی می‌شوند ولی این لزوماً مربوط به عناصر اصلی فرهنگ ما نمی‌شود بلکه تغییر در لایه‌ای از فرهنگ رخ می‌دهد که لایه‌ای متنوع و

متکثر است (نقیب‌زاده، ۱۳۸۸: ۱۶۸)؛ بنابراین، باید یاد بگیریم که خود را با آن به صورت خلاقانه‌ای تطبیق داده و نوعی انعطاف‌پذیری فرهنگی داشته باشیم؛ ضمن آنکه فناوری‌های نوین می‌توانند حوزه‌ای عالی برای دفاع از ارزش‌ها در مقابل تهاجم‌های فرهنگی باشند. بهره‌گیری از فرهنگ ایرانی - اسلامی به عنوان منبعی از قدرت نرم نیز در همین راستا قابل بررسی است.

۷. توسعه سیاسی و بازتولید نسلی پشتیبان از طریق گسترش مردم‌سالاری دینی: یکی از ملزومات مهم قدرت ملی کشورها نحوه و میزان حمایت‌های مردمی از حکومت و آرمان‌های آن در بین مردم است (افتخاری و دیگران، ۱۳۸۹: ۲۸۴). هرچند در جریان پیروزی انقلاب اسلامی و هشت سال دفاع مقدس، اوج حمایت مردم از نظام سیاسی را شاهد بودیم ولی در برخی مقاطع زمانی، این روند دستخوش دگرگونی‌هایی شد که پیامدهای آن به صورت بازخوردی منفی در فضای مجازی مشاهده می‌شد. جمهوری اسلامی ایران باید بتواند از طریق توسعه سیاسی که امکان مشارکت سیاسی را برای تمامی افراد و تولید رضایت در میان آنها فراهم می‌سازد، نسلی پشتیبان از مبانی مردم‌سالاری دینی پرورش دهد.

۸. حفاظت از زیرساخت‌ها: هرچند 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. در این راستا طیفی از اقدامات می‌تواند مورد بررسی قرار گیرد: مشخص کردن سطح فعلی حفاظت از زیرساخت‌ها و درجه ریسک آنها؛ فهم کاملی از اینکه دقیقاً چه کسانی بر کدام بخش‌ها کنترل و حق اقدام دارند؛ افزایش آگاهی ملی از طریق آموزش؛ و ایجاد درجه‌ای از همکاری بین‌المللی برای مقابله با تهدیدها و تعقیب مجرمان سایبری (هالپین و دیگران، ۱۳۸۹: ۳۸۹).



### پی‌نوشت‌ها

۱. جمهوری اسلامی ایران با بیش از ۴۲ میلیون کاربر، در فهرست ۲۰ کشور اول جهان از نظر تعداد کاربر اینترنت است و در میان کشورهای خاورمیانه نیز مقام اول را داراست. در بازار تلفن همراه نیز در میان ۲۰ کشور اول جهان و در خاورمیانه نیز بعد از ترکیه در مقام دوم قرار گرفته است. [www.internetworldstats.com](http://www.internetworldstats.com) – June 30, 2012
2. Eriksson, J. (2007), *International Relation and Recurity in Digital Age*, Routledge.
3. Kshetri, N. (2005), “Information and Communications Technologies, Strategic Asymmetry and National Security”, *Journal of International Management*, Vol. 11, September 14.
4. Goldman, E. (2004), *National Security in Information Age*, Frank Cass.
5. Mazarr, M. (2005), *Information Technology and World Politics*, First published by Palgrave Macmilan, Hampshire.
۶. جیمز روزنا و سینگ (۱۳۹۱)، *فناوری اطلاعات و سیاست جهانی*، مترجم: احمد سلطانی‌نژاد و احمد محقر، چاپ اول، تهران: انتشارات دانشگاه امام صادق(ع).
۷. اینترنت ۵۰ میلیون مخاطب را تنها در مدت چهار سال جذب کرد.
۸. برای اطلاعات بیشتر ر.ک. به:
- حافظ‌نیا و همکاران، «تأثیر جهانی‌شدن بر هویت ملی»، *فصلنامه ژئوپلیتیک*، سال دوم، شماره ۳ و ۴.
- عباسی قادری و خلیلی کاشانی (۱۳۸۹)، *تأثیر اینترنت بر هویت ملی*، تهران: پژوهشکده مطالعات راهبردی.
9. [www.kurdishamerican.org](http://www.kurdishamerican.org)
۱۰. براساس این دیدگاه افزایش دسترسی مردم در داخل به فناوری‌های اطلاعات و مقابله با سانسور و فیلترینگ، یکی از عوامل مهم در تسریع تغییرات سیاسی است.
۱۱. استارس در برابر استارکس‌نت، ۶ اردیبهشت ۹۰: <http://irdiplomacy.ir>

۱۲. USB استاکس نت؛ نگاهی به بمباران مجازی تأسیسات هسته‌ای ایران، ۲۹/۰۸/۲۰۱۱:  
[www.dw.de/dw/article](http://www.dw.de/dw/article)
۱۳. پهنای باند، حجم اطلاعاتی است که می‌توان در هر زمان مشخص از یک دستگاه رله فرستاد.
۱۴. نوکیا زیمنس: فروش تجهیزات به ایران را متوقف کرده‌ایم. ۱۵ مهر ۸۹: [www.Aftabnews.ir](http://www.Aftabnews.ir)
15. [www.israel.org](http://www.israel.org)

## منابع

- احمدیان، قدرت (۱۳۸۰)، «انقلاب اطلاعات و تحول مفهوم امنیت»، *فصلنامه رسانه*، سال یازدهم، شماره اول.
- افتخاری، اصغر (۱۳۷۹)، «امنیت در حال گذار؛ تحول معنای امنیت در قرن بیستم»، *فصلنامه مطالعات راهبردی*، سال سوم، شماره ۴.
- افتخاری، اصغر و دیگران (۱۳۸۹)، *قدرت نرم، فرهنگ و امنیت (مطالعه موردی بسیج)*، چاپ دوم، تهران: دانشگاه امام صادق (ع).
- بوزان، باری (۱۳۷۸)، *مردم، دولت‌ها و هراس*، مترجم: پژوهشگران پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.
- بهمن، شعیب (۱۳۸۹)، «جنگ سایبری امریکا و رژیم صهیونیستی علیه ایران»، *روزنامه همشهری*، شنبه ۸ آبان.
- پورسعید، فرزاد (۱۳۸۸)، «بازتولید گفتمانی؛ راهبرد استقرار امنیت نرم در جامعه ایرانی»، *فصلنامه مطالعات راهبردی*، سال ۱۲، شماره ۳.
- تاجیک، محمدرضا (۱۳۸۱)، *مقدمه‌ای بر استراتژی‌های امنیت ملی*، جلد اول: *رهیافت‌ها و راهبردها*، چاپ اول، تهران: انتشارات فرهنگ گفتمان.
- تافلر، آلوین (۱۳۷۶)، *به سوی تمدن جدید*، مترجم: محمدرضا جعفری، تهران: سیم‌غ.
- چین، زوئینگ (۱۳۸۵)، «فناوری نرم و نسل چهارم آینده‌نگاری فناوری»، مترجم: محمدرضا میرزا امینی، *فصلنامه رشد فناوری*، شماره ۸، سال دوم، صص ۴۸-۵۶.
- رحمت‌اللهی، حسین (۱۳۸۴)، «جهانی‌شدن و تأثیر آن بر هویت‌های قومی و ملی»، *اندیشه‌های حقوقی*، سال سوم، شماره ۸، صص ۹۱-۱۱۱.
- روزنا و سینگ (۱۳۹۱)، *فناوری اطلاعات و سیاست جهانی*، مترجم: احمد سلطانی‌نژاد و احمد محقر، چاپ اول، تهران: دانشگاه امام صادق (ع) (زیر چاپ).
- روزنا، جیمز (۱۳۸۴)، *آشوب در سیاست جهان*، مترجم: علیرضا طیب، چاپ اول، تهران: روزنه.
- روزنا، جیمز و دیگران (۱۳۹۰)، *انقلاب اطلاعات، امنیت و فناوری‌های جدید*، مترجم: علیرضا



- طیب، چاپ اول، تهران: پژوهشکده مطالعات راهبردی.
- صالحی امیری، سید رضا، شهرود انتخابی و محمد سلطانی فر (۱۳۸۷)، *دیپلماسی رسانه‌ایی*، چاپ اول، تهران: گروه پژوهش‌های فرهنگی و اجتماعی مجمع تشخیص مصلحت نظام.
- ضیایی پرور، حمید (۱۳۹۰)، «پیامدهای قطع پیامک»، *روزنامه همشهری*، ۱۲ آذر.
- قاسم‌زاده، فریدون (۱۳۷۹)، *آشنایی با اینترنت و تجارت الکترونیک*، تهران: انستیتو ایز ایران.
- کاستلز، امانوئل (۱۳۸۰)، *عصر اطلاعات: اقتصاد، جامعه و فرهنگ*، ظهور جامعه شبکه‌ای، جلد ۱، مترجم: احمد علیقلیان، افشین خاکباز، چاپ دوم، تهران: طرح نو.
- مجموعه مقالات، *ارزیابی‌های انتقادی در زمینه امنیت بین‌الملل* (۱۳۸۰)، گردآوری و مترجم: علیرضا طیب، چاپ اول، تهران: نی.
- مجموعه مقالات، *تکنولوژی اطلاعات* (۱۳۸۹)، گردآوری و مترجم: علیرضا طیب، چاپ اول، تهران: سفیر.
- مطهرنیا، مهدی (۱۳۸۱)، «آشوب در جهان؛ انقلاب اسلامی در ایران»، *فصلنامه انقلاب اسلامی*، تهران: سال اول، شماره ۴.
- میناوندچال، محمدقلی (۱۳۸۱)، *بررسی قابلیت و امکان عملکرد اینترنت به عنوان حوزه عمومی سیاسی*، رساله دکتری علوم سیاسی، دانشگاه تربیت مدرس.
- نای، جوزف (۱۳۸۹)، *قدرت نرم: ابزارهای موفقیت در سیاست بین‌الملل*، مترجم: سید حسن روحانی و مهدی ذوالفقاری، چاپ سوم، تهران: دانشگاه امام صادق (ع).
- نقیب‌زاده، احمد (۱۳۸۸)، *تأثیر فرهنگ ملی بر سیاست خارجی جمهوری اسلامی ایران*، چاپ اول، تهران: دفتر مطالعات سیاسی و بین‌المللی وزارت خارجه.
- هالپین و دیگران (۱۳۸۹)، *جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی*، مترجم: روح‌الله طالبی آرانی، چاپ اول، تهران: مرکز پژوهش‌های مجلس شورای اسلامی.
- Alberts & Papp (1997), *Information Age Anthology: National Security Implications of the Information Age*, US, published in National Defense University by NDU press and DOD CCRP Publications
- Albright, Paul Brannan, and Christina Walrond (2010), *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*, December 22, , <http://isis-online.org>
- Dumbrell, J. (2007), *The Bush Administration, US Public Diplomacy and Iran*, Working Paper. Durham University, School of Government and International Affairs.
- E. Price. M. (2002), *Media and Sovereignty: the Global Information Revolution and its*

- Challenge to State Power*, USA, by Massachusetts Institute of Technology.
- Eriksson. J., (2009), "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State", *International Studies Review*, Vol. 11.
- G. Patman. R. (2006), *Globalization and Conflict, National Security in New Strategic Era*, first published, UK, by Routledge.
- Grossman L. (2009), *Iran's Protest: Why Twitter Is the Medium of the Movement*, 17 June 2009: <http://www.time.com>
- G. Patman. R. (2006), *Globalization and Conflict, National Security in New a Strategic Era*, first published, UK, by Routledge.
- J. Mazarr. M. (2005), *Information Technology and World Politics*, First published, Hampshire, by Palgrave Macmilan.
- Kirshner, J. (2006), *Globalization and National Security*, London: Taylor and Francis group.
- Mina N. (2007), Blogs, Cyber-Literature and Virtual Culture in Iran, *George C. Marshall European Center for Security Studies*, December, No. 15.
- Nafisi, A. (2008), *Blogging Outside Iran: A Tool for Internal Democratic Change*, Thesis advisor, US: University of Washington's Department of Communication Honors Program.
- Rahimi B. (2003), "Cyber Dissent: the Internet in Revolutionary Iran", *Middle East Review of International Affairs*, Vol. 7, September, No. 3.
- Ritzer G. (2007), *The Blackwell Companion to Globalization*, Blackwell publishing.
- Shirky. C. (2011), "The Political Power of Social Media, the Technology, the Public Sphere and Political Change", *Foreign Affairs*, January/February, Vol. 90, No. 1.
- S. Nye, J. (2002), "The Information Revolution and American Soft Power", *Asia-Pacific Review*, Vol. 9, Issue 1.
- S. Nye, J. (2011), "The Future of Power", *Bulletin of the American Academy of Art Sciences*, Spring, Vol. LXIV, Issue 3, pp. 45-52.
- Solymar L. (1999), *Getting the Message: A history of Communications*, first published, UK, Oxford University Press.