شاخص‌های فناوری اطلاعات و ارتباطات در امنیت داخلی جمهوری اسلامی ایران

اسماعیل کرم زاده[1]

تاریخ دریافت: ۱۳۹۳/۱۲/۰۴
تاریخ پذیرش: ۱۳۹۳/۰۳/۲۳

چکیده

رشد روزافزون فناوری اطلاعات و ارتباطات در عصر کنونی موجب گردیده کلیه عرصه‌های جامعه شامل؛ حوزه‌های سیاسی، اقتصادی، اجتماعی و فرهنگی، تحت‌تأثیر قرار گرفته و در این میان حوزه امنیت نیز بی‌نصیب نمانده است. از طرفی؛ وجود تهدیدها و آسیب‌های موجود در امنیت داخلی که ممکن است موجب بی‌ثباتی و ناامنی گردد و دسترسی آسان به فناوری و حوزه‌هایی که قبلاً در اختیار سازمان‌های امنیتی بوده، موجب شده تا هم‌زمان تهدیدها نیز شکل بدیع‌تری پیدا کرده و این امر باعث شد که سطح دسترسی افراد و بازیگران فاقد صلاحیت، به اطلاعات طبقه‌بندی شده افزایش یابد. از این رو بخش اعظمی از تهدیدهای امنیتی با استفاده از فناوری اطلاعات و ارتباطات صورت می‌پذیرد که امروزه تأمین امنیت داخلی و طراحی و هدایت محیط‌های امنیتی و مقابله با تهدیدهای امنیت داخلی، بدون استفاده از فناوری و تکنولوژی‌های مورد نیاز، ممکن نیست.

در این مقاله ضمن بررسی تأثیر فناوری بر امنیت داخلی جمهوری اسلامی ایران و نقش آن در شناخت و کنترل محیط‌های امنیتی، در نهایت شاخص‌های فناوری اطلاعات و ارتباطات در امنیت داخلی بیان می‌گردد.

روش تحقیق در این مقاله؛ توصیفی و جمع‌آوری داده‌ها به روش کتابخانه‌ای و اسنادی و مصاحبه انجام شده که با استفاده از روش تحلیل گفتمان، نتیجه‌گیری و شاخص‌های فناوری امنیت داخلی بیان شده است.

نتایج حاصله بیا نگر این است که شاخص‌های ارتقاء روش‌های جمع‌آوری اطلاعات، افزایش تولید اطلاعات راهبردی، افزایش شناخت نسبت به تأثیر پدیده‌ها، کیفیت و دقت در شناخت تهدید، ارتقاء توانایی در اتخاذ اقدام هدفمند، تقویت بررسی، تحلیل و ارزیابی امنیتی، شناسایی نقاط قوت و ضعف و تهدید، کسب مهارت‌های هوشمند در مبارزه با تهدیدهای امنیتی، از مهم‌ترین شاخص‌های فناوری اطلاعات و ارتباطات در امنیت داخلی می‌باشد.

کلید واژه‌ها:

شاخص/ فناوری اطلاعات و ارتباطات/ امنیت داخلی/ فناوری.

---

۱. دانشجوی دکتری امنیت داخلی دانشگاه عالی دفاع ملی

مقدمه

فناوری، به نحوی پیچیده و بغرنج با زندگی انسان در آمیخته است؛ طوری که ما اغلب حضور آن را در همه‌جا احساس می‌کنیم. اگر با دقت به اطراف خود نگاه کنیم، متوجه می‌شویم که در طول سالیان متمادی، فناوری راه خود را به سوی اکثر جنبه‌های زندگی انسان پیدا کرده است.

عصر اطلاعات و ارتباطات، دوره نوینی در سیر تطور و تکامل جوامع بشری است که در آن با پیشرفت علوم و فناوری، اطلاعات وسیعی در دسترس انسان‌ها قرار گرفته است. طوری که به تناسب توانایی در تجزیه و تحلیل این اطلاعات، امکان دستیابی به سطوح عالی‌تری از دانش برای آنها فراهم شده است. بنابراین، می‌توان قدرت فناوری و ارتباطات را به‌مثابه یک شاخص مهم توسعه در کنار سایر مؤلفه‌های قدرت ملی مورد تأکید قرار داد. از طرفی؛ افزایش اقتدار و امنیت، باید هماهنگ با اقتدار نیروهای کنترلی و حمایتی در جهت آزادی عمل و تفکر شهروندان و احساس اعتماد متقابل و مشارکت عمومی پایدار، شکل گیرد.

ایجاد، حفظ و پایداری امنیت، نیازمند مشارکت و هم‌دلی و هم‌اندیشی تمام لایه‌ها و ساختارها و گروه‌های اجتماعی است. برای ارتقاء امنیت و احساس آن، نیازمند سیاستگذاری سنجیده و برنامه‌ریزی دقیق و اقدامات مؤثر و دخالت دادن وجه نرم‌افزاری مدیریت امنیتی هستیم که بتواند به پایداری و فراگیری امنیت کمک کند.

بنابراین، ضرورت کنترل آسیب در حوزه امنیت داخلی، شناخت علمی آنها را برای پاسخ به پرسش‌های نظری و عملی و کاربردی از ایده‌ها و یافته‌های علمی تولید شده و برنامه‌ریزی کوتاه و بلندمدت برای مقابله صحیح با آسیب‌ها، درمان و یا پیشگیری از گسترش آنها نیز ضروری و پراهمیت می‌سازد.

آسیب‌های اجتماعی امنیت، در صورت عدم کنترل به سهولت هرج و مرج، آسیب و بحران‌های حادث را در لایه‌های مختلف جامعه پراکنده می‌کنند و حتی به وجود می‌آورند. بنابراین، ضرورت و اهمیت بررسی علمی و دقیق ظرفیت‌ها و پتانسیل‌های آسیب‌زا جهت شناخت عوامل تأثیرگذار بر کنترل آسیب‌های اجتماعی امنیت، نمایان‌تر می‌شود. از این‌رو، می‌توان با بهره‌گیری از قدرت فناوری اطلاعات و ارتباطات و برخورداری از دستاوردهای دانش نوین در این زمینه، از آن به عنوان یک شاخص مهم توسعه در کنار سایر مؤلفه‌های قدرت ملی در تأمین امنیت داخلی جمهوری اسلامی ایران استفاده نمود.

در این مقاله، تلاش کرده‌ایم که با تبیین دو مبحث مهم «فناوری اطلاعات و ارتباطات» و «امنیت داخلی»، به بیان شاخص‌های فناوری در امنیت داخلی جمهوری اسلامی ایران بپردازیم و در واقع سؤال اصلی این مقاله، این است که شاخص‌های فناوری اطلاعات و ارتباطات در امنیت داخلی جمهوری اسلامی ایران کدامند؟

الف. کلیات

۱/الف. بیان مسئله:

رشد روزافزون فناوری اطلاعات و ارتباطات در عصر کنونی موجب گردیده کلیه عرصه‌های جامعه شامل؛ حوزه‌های سیاسی، اقتصادی، اجتماعی و فرهنگی، تحت‌تأثیر قرار گرفته و در این میان، حوزه امنیت نیز بی‌نصیب نمانده است. تأمین امنیت داخلی بدون استفاده از فناوری اطلاعات و ارتباطات محقق نمی‌گردد؛ چرا که بخش اعظمی از تهدیدهای امنیتی با استفاده از فناوری اطلاعات و ارتباطات صورت می‌پذیرد.

در عصر کنونی، اطلاعات و ارتباطات از عوامل بسیار مهم کسب قدرت و تأمین امنیت می‌باشد. امروزه دشمن با استفاده از این فناوری، از مرزهای سیاسی و اجتماعی و فرهنگی و اعتقادی و ازجمله امنیتی کشورهای هدف می‌گذرد و کشوری که در استفاده از این فناوری برای مقابله با این تهدیدها آماده نباشد، مسلماً نمی‌تواند امنیت خود را حفظ نماید. اگر این نکته را بپذیریم که دستیابی به آخرین فناوری اطلاعات و ارتباطات و استفاده از آن در تأمین امنیت داخلی الزامی می‌باشد، باید بتوانیم که شاخص‌های آن را در تأمین امنیت داخلی مشخص نماییم. در واقع تعیین شاخص‌ها، نیازمندی‌های کسب چنین فناوری را مشخص می‌سازند.

بدیهی است فناوری اطلاعات و ارتباطات، در زمره عناصر قدرت‌زا همواره مورد سوءاستفاده دشمنان امنیت داخلی قرار گرفته و از آنجا که نظام مقدس جمهوری اسلامی ایران همواره از بدو تأسیس تا کنون، مورد هجوم انواع تهدیدهای سخت و نرم استکبار جهانی واقع شده است، لذا دشمن تلاش می‌کند با استفاده از برتری اطلاعاتی و ارتباطی، با هدایت جریان‌های سیاسی، فرهنگی و اجتماعی ضدنظام، بتواند در تفکر، سازماندهی، هدف‌ها، نیات مردم و مسئولین نظام مقدس جمهوری اسلامی ایران خلل ایجاد نماید.

بنابراین، در این پژوهش تلاش می‌گردد شاخص‌های فناوری اطلاعات و ارتباطات در امنیت داخلی را مشخص نماییم. امید است این مطالعه، مقدمه‌ای برای انجام مطالعات تکمیلی در این حوزه گردد.

۲/الف. اهمیت و ضرورت تحقیق:

کاهش نقش‌آفرینی فواصل زمانی و مکانی و تعاملات انسانی در عصر اطلاعات و ارتباطات، سبب گردیده کنترل اطلاعات و ارتباطات، به امری پیچیده و دشوار بدل گردد. دشواری کنترل اطلاعات و ارتباطات، موجب بروز مخاطرات جدیدی در ابعاد امنیت داخلی می‌گردد.

افزایش سرعت توزیع اطلاعات، افزایش دسترسی به اطلاعات و ارتباطات، افزایش انعطاف‌پذیری گردش اطلاعات و ارتباطات و افزایش ظرفیت انتقال اطلاعات و

ارتباطات، در زمره اصلی‌ترین عوامل دشواری کنترل اطلاعات و ارتباطات محسوب می‌شوند. این حوزه به عنوان اصلی‌ترین سازنده و در حقیقت سنگ بنای قدرت نرم کشورها، از یک کاربری سیاسی به منظور نیل به هدف‌های سیاسی و امنیتی برخوردار می‌گردد.

وجود تهدیدها و آسیب‌های موجود در امنیت داخلی که ممکن است موجب بی‌ثباتی و ناامنی گردد و از طرفی؛ رشد روزافزون فناوری اطلاعات و ارتباطات و استفاده از این فناوری در تمامی عرصه‌ها و ظهور بازیگران متعدد و دسترسی آنان به فناوری و حوزه‌هایی که قبلاً در اختیار سازمان‌های امنیتی بوده‌اند، موجب شده هم‌زمان تهدیدها نیز شکل بدیع‌تری پیدا کند. همچنین این امر باعث شده تا دسترسی افراد و بازیگران فاقد صلاحیت، به اطلاعات طبقه‌بندی شده افزایش یابد. از این‌رو، برای استفاده از فناوری ارتباطات و اطلاعات در تأمین امنیت داخلی، می‌طلبد که شاخص‌های فناوری در این عرصه که موضوع مقاله کنونی می‌باشد، مشخص گردد.

۳/الف. هدف اصلی تحقیق:

تعیین شاخص‌های فناوری اطلاعات و ارتباطات در تأمین امنیت داخلی.

۴/الف. سؤال اصلی تحقیق:

شاخص‌های فناوری اطلاعات و ارتباطات در تأمین امنیت داخلی جمهوری اسلامی ایران کدامند؟

۵/الف. روش تحقیق و ابزار گردآوری اطلاعات:

این تحقیق از نوع کاربردی است. در این تحقیق، داده‌های مورد نیاز با استفاده از روش مطالعه اسنادی و کتابخانه‌ای، جمع‌آوری و از ابزار فیش‌برداری و مصاحبه عمیق و تحلیل گفتمانی استفاده شده است.

۶/الف. جامعه و نمونه آماری:

با تعداد ۱۵ نفر از خبرگان در حوزه امنیت و فناوری اطلاعات و ارتباطات مصاحبه عمیق صورت پذیرفت. از این تعداد، ۵ نفر از اساتید رشته امنیت داخلی و ۴ نفر از اساتید سایبری و ۶ نفر از مدیران اجرایی ناجا، در پلیس‌های تخصصی و فاواناجا می‌باشند.

ب. ادبیات نظری

۱/ب. مفهوم فناوری:

در دنیای امروز یکی از عناصر اصلی تشکیل‌دهنده قدرت اعم از قدرت سیاسی، اقتصادی، نظامی، فرهنگی و اطلاعاتی، مسئله فناوری برتر است که به مولد قدرت تبدیل شده است.

به‌کارگیری هدفمند معرفت علمی برای منظورهای عملی یا تولیدی، از جمله هدف‌های فناوری است. از این‌رو، برخی فناوری را روشی تکنیکی برای کسب و نیل به هدف‌های عملی می‌دانند. از نظر هایدگر، برآوردن تمایلات و هدف‌ها با استفاده از امکانات و وسایل، نوعی فعالیت انسانی است (هایدگر، ۱۳۷۵: ۹۲).

سرعت در تحولات تکنولوژی، منعکس‌کننده و تقویت‌کننده سطوح کامل از ساختار اجتماعی است. جوامع پیشرفته بسیار بیشتر از آنچه تا قبل از پیدایش آنها ممکن بوده است، انرژی‌های سازنده را در انواع مختلف آن از محیط ملی خود استخراج کرده‌اند. این عامل سازمانی، به همان اندازه بعد سخت‌افزاری انقلاب فناورانه، به قدرت کشورِ دارنده آن کمک می‌رساند (بوزان، ۱۳۷۷: ۵۶).

در طول تاریخ با تأکید بر دو رویکرد مختلف، به تعریف فناوری پرداخته شده است. این دو رویکرد عبارتند از: ۱. رویکرد درون‌گرایان[۱] ۲. رویکرد برون‌گرایان.[۲]

---

۱ . internalists

۲ . externalist

تعاریف درون‌گرایان از فناوری، اغلب با تکیه بر معنی و مفهوم مهندسی آن؛ یعنی ساختن مصنوعات و استفاده کردن از آنها بوده است. برای مثال؛ کرانزبرگ[۱] و پورسل[۲] فناوری را چنین تعریف می‌کنند: «تلاش انسان برای مواجه شدن با محیط فیزیکی... و ملی، برای رام کردن یا کنترل کردن محیط به‌وسیله... ابتکار و نبوغ خود در استفاده نمودن از تمامی منابع در دسترس» (Mitcham, ۱۹۹۴: ۱۱۶).

از سوی دیگر؛ تعاریف ارائه شدهٔ برون‌گرایان از فناوری، بر پایه اثراتی بوده که بر روی نهادهای اجتماعی گذاشته است. از این رو، اغلب صاحب‌نظرانِ این دیدگاه را دانشمندان علوم اجتماعی تشکیل می‌دهند. برای مثال؛ «سینگر» فناوری را چنین تعریف می‌کند: «اینکه هر چیزی به طور معمول چگونه انجام می‌شود؛ یا ایجاد می‌شود و اینکه چقدر انجام می‌شود و یا ایجاد می‌شود» (همان).

امروزه تعاریفی که از فناوری ارائه می‌شود، معمولاً تلفیقی از هر دو دیدگاه مهندسی و اجتماعی می‌باشد که یکی از این تعاریف، عبارت است از: مجموعه‌ای متشکل از اطلاعات، ابزارها و تکنیک‌هایی که از علم و تجربه عملی نشئت گرفته‌اند و از توسعه، طراحی، تولید و به‌کارگیری محصولات، فرآیندها، سیستم‌ها و خدمات، مورد استفاده قرار می‌گیرند.

اما از دیدگاه اجتماعی، فناوری عبارت است از همه فرآیندها، روش‌ها، فنون، معلومات و همچنین مصنوعاتی که جامعه را در حفظ، بقا و ارتقای خود یاری می‌دهد (جعفرنژاد، ۱۳۸۸: ۹۰).

در تعاریف جدید، سه مؤلفه طرح‌های تولیدی، تکنیک‌های تولید و حتی عملکردهای مدیریتی نیز جزء فناوری محسوب شده‌اند. از این‌رو، عمل مدیریتی در جامعه و سازمان‌ها، می‌تواند بخشی از فناوری به‌شمار آید (Howard & Sagafinejad,۱۹۸۱:chap۱).

---

۱ . kernazberg

۲ . porsel

از این رو، در عصر فناوری، شکل‌های منازعه و ویژگی‌های تهدیدها میان کنشگران تغییر یافته است. فناوری بر توانمندی نظامی، اطلاعاتی، سیاسی و اقتصادی بازیگران بین‌المللی که برای بقا و امنیت تلاش می‌کنند، تأثیر می‌گذارد. ضمن اینکه ماهیت تهدیدها را دگرگون ساخته و عرصه‌های نوینی را در برابر کنشگران باز می‌کند (نورمحمدی، ۱۳۹۰: ۴۴).

بهره‌گیری از دانش و فنون بشری برای تأمین منافع ملی نظام سیاسی، در طول تاریخ هدف سیاستمداران و مسئولان امنیتی کشورها بوده است. فناوری نوین در عرصه ارتباطات و اطلاعات، موجب گردیده که انقلاب عظیمی در افزایش خبر و اطلاعات پدید آید. انقلاب رایانه‌ای و انقلاب اینترنتی، شیوه‌های تولید، انباشت و بازیابی داده‌ها را متحول کرد و بدین ترتیب، ماهیت تعاملات میان لایه‌های مختلف جامعه را تغییر داد.

امروزه توسعه فناوری اطلاعات و ارتباطات، موجب شده دستگاه‌های امنیتی و اطلاعاتی با بهره‌گیری از این پدیده در مأموریت‌ها و عملیات‌های مختلف، کاربرد آن را به بخش انکارناپذیر در فعالیت‌های اطلاعاتی بدل نمایند. روند پیدایش مفهوم فناوری، گذشته از تعاریف فوق، تاکنون شامل پنج مرحله بوده که عبارتند از:

۱. دوره انقلاب صنعتی و مکانیزاسیون اولیه (از سال ۱۷۷۰ تا ۱۸۳۰) که ناظر به شکوفایی صنایع نساجی، ذوب آهن و ریخته‌گری بود؛
۲. دوره تاریخی بخار و ماشین‌آلات و تجهیزات بخار (از سال ۱۸۳۰ تا ۱۸۸۰) که موجب تولید ماشین‌سازی، کشتی‌های بخار و تجهیزات راه‌آهن گردید؛
۳. دوره مهندسی برق و صنایع سنگین (از سال ۱۸۸۰ تا ۱۹۳۰) که در این دوره مهندسی برق، تجهیزات و ماشین‌آلات برقی، کابل و سیم، مهندسی سنگین کشتی‌های فولادی و مواد شیمیایی و موضوعی، عمده‌ترین زمینه‌های برتری بازیگران بوده است؛
۴. دوره فوردیستی و تولید انبوه (از ۱۹۳۰ تا ۱۹۸۰) که صنایع خودروسازی و هواپیماسازی، اهمیت فوق‌العاده‌ای می‌یابند؛

۵. دوره فناوری اطلاعات و ارتباطات (از ۱۹۸۰ به بعد) که اکنون در آن به‌سر می‌بریم. در این دوره، رایانه، محصولات الکترونیکی، نرم‌افزارها و تجهیزات مخابراتی، فیبر نوری، ربات‌ها و نیمه‌هادی‌ها، عمده‌ترین فناوری‌های رشدیابنده است که هم‌اکنون با رشد فزاینده‌ای در عرصه فناوری‌های نوین به‌سر می‌بریم. دانشمندان بر این عقیده هستند که دوره بعدی، دوره نانوفناوری و مهندسی ژنتیک است و رشته‌های رشدیابنده در این دوره عبارتند از بیوفناوری، شیمی دقیق و هوا – فضا که ممکن است در آینده‌ای نه‌چندان دور، پارادایم جدیدی را به جهان و جهانیان معرفی کنند (جعفرنژاد، ۱۳۸۸، ۱۰۰-۹۱).

فناوری در این مرحله، فرآیندی است که در آن اطلاعات، پول، خدمات، کالاها، قدرت، سرگرمی‌ها، طرز رفتار، افکار، ارزش‌ها و مانند آن، در مقیاس جهانی معنا می‌یابد (توکل، ۱۳۹۰: ۴۴).

فناوری اطلاعات و ارتباطات، بر توانمندی‌های نظامی، امنیتی، سیاسی و اقتصادی بازیگران ملی و بین‌المللی که برای امنیت تلاش می‌کنند، تأثیر می‌گذارد. ضمن اینکه ماهیت تهدیدها را دگرگون ساخته و عرصه‌های نوینی را در برابر کنشگران باز می‌کند (نای، ۱۳۹۰: ۳۷۷).

تحولات ناشی از ظهور گسترده فناوری اطلاعات و ارتباطات را می‌توان به یک پدیده تشبیه کرد. پدیده، اثری ابداعی و شامل چندین عامل و متغیر است که رخداد ناشی از تبعاتی پیچیده و ناشناخته دربر دارد. مطالعه این پدیده، از نظر ویژگی‌ها و متغیرهای شکل‌دهنده آن، حائز اهمیت است. در ادامه به برخی از ویژگی‌های فناوری اطلاعات و ارتباطات اشاره می‌کنیم.

۲/ب. مفهوم فناوری اطلاعات و ارتباطات:

تاکنون تعاریف گوناگونی از فناوری اطلاعات و ارتباطات ارائه شده که این امر دستیابی به تعریفی فراگیر و برداشتی واحد را دشوار کرده است. اما در یک تعریف کلی

با توجه به مفهوم فناوری (که در این مقاله به آن اشاره شد)، «مجموعه‌هایی از روش‌ها و فناوری‌هایی که به منظور تسهیل و انجام فرآیند تولید، گردآوری، سازماندهی، ذخیره، بازیابی و نشر اطلاعات به‌کار گرفته می‌شوند، منوط به داشتن دو شرط اساسی یعنی استفاده از رایانه به عنوان ابزار پردازش و ارتباطات به عنوان شاه‌راه ارتباطی، فناوری اطلاعات و ارتباطات گفته می‌شود» (فناوری و قدرت ملی، ۱۳۸۸: ۴۶).

۳/ب. ویژگی‌های فناوری اطلاعات و ارتباطات:

۱. موجب تحول و انقلاب: این فناوری موجب تحول و انقلاب در عصر بشر گردیده است. به نوعی این انقلاب را می‌توان به تعبیر «تافلر» انقلاب سوم و یا حتی شاید آخرین موج تمدن بشری نیز دانست؛

۲. عامل تجدید قدرت: فناوری اطلاعات و ارتباطات منابع و فرآیندهای تولید، تغییر و جریان قدرت را متحول نموده است. این فناوری امروزه ابزار اداره و تسخیر دنیا و جهانی‌سازی است؛

۳. عامل دگرگونی انگاره‌ها و الگوهای ذهنی: بخش اعظمی از تحولات ناشی از فناوری اطلاعات و ارتباطات در سال‌های اخیر ناشی از شکل‌گیری الگوهای ذهنی جدید، مبانی تحلیل و تفکر جدید و مدل‌های رفتاری نوین بوده است؛

۴. فرصت‌های طلایی در کنار تمهیدات همه‌جانبه: فناوری اطلاعات همچون شمشیری دو لبه، از یک طرف می‌تواند فرصت‌های طلایی را برای جبران عقب‌ماندگی‌ها فراهم آورد و رشد و توسعه را به شکل باورنکردنی هموار نماید و از طرف دیگر؛ موجب می‌شود تهدیدهایی با شکل جدید که گاهی ناشناخته و بسیار اثربخش هستند، گردیده که لازمه هرگونه اقدام در توسعه این فناوری، شناخت و کشف این تهدیدها و اتخاذ تدابیر لازم در قبال آنها است؛

۵. فناوری اطلاعات و ارتباطات به عنوان میدان نبرد جدید، از مجموعه عوامل تغییر ماهیت جنگ‌های مدرن محسوب می‌شوند و مفاهیم مشابه چون امنیت ملی و سیاست‌های ملی نیز تغییرهای محسوسی را شاهد خواهند بود.

عوامل فوق از ویژگی‌های مهم فناوری اطلاعات و ارتباطات در عرصه قدرت و امنیت کشورها می‌باشند که علاوه بر ویژگی‌های فوق، به سایر ویژگی‌ها نیز می‌توان اشاره کرد که عبارتند از:

۱. افزایش عملکرد بخش‌های تولیدی؛
۲. افزایش سرعت ارائه خدمات؛
۳. افزایش دقت انجام کارها؛
۴. کاهش هزینه سازمان‌ها؛
۵. کاهش مفاسد اداری و مفاسد اقتصادی؛
۶. اطلاع‌رسانی و آگاهی مردم از فرصت‌ها؛
۷. کاهش مفاسد اداری و مفاسد اقتصادی؛
۸. اطلاع‌رسانی و آگاهی مردم از فرصت‌ها؛
۹. ایجاد امکان و شرایط کار تمام وقت از طریق شبکه‌های رایانه‌ای؛
۱۰. ایجاد امکان همکاری از راه دور؛
۱۱. کمک به مدیریت بهتر و ده‌ها ویژگی دیگر که از حوصله این مقاله خارج است.

چنین ویژگی‌هایی از فناوری و به‌خصوص فناوری اطلاعات و ارتباطات، موجب تأثیرهای عمیق در حوزه فعالیت‌های امنیتی گردیده است. درک نقش فناوری در فعالیت‌ها و توانایی‌های امنیتی، می‌تواند موجب تحول در شرح وظایف بنیادین نهادها و بالطبع دستیابی به امنیت پایدارتر در عرصه امنیت داخلی گردد.

۴/ب. مفهوم امنیت داخلی:

امنیت، قوام‌بخش و تعیین‌کننده توسعه و تعاملات اجتماعی است. زیستن افراد در کنار هم و پیشبرد هدف‌ها، به امنیت نیاز دارد. وضعیت، استحکام، قدرت و بنیان‌های ساختارهای داخلی یک جامعه، به امنیت آن وابسته است. در گفتمان مردم‌سالاری و در منطق مملکت‌داری در عصر جدید، نکته اصلی؛ ربط و وثیق امنیت به کارکردها و ساختارهای اجتماعی است که هم افراد در آن نقش دارند و هم منافع نهادها، احزاب، تشکیلات صنفی و نیز سیاست‌های سازمان‌یافته، اولویت دارند. امنیتی که به ساختارهای داخلی متکی نبوده و مورد حمایت شهروندان نباشد، آسیب‌پذیر است.

از دیرباز، یکی از شاخص‌های اصلی مشروعیت و کارآمدی نظام سیاسی، میزان بهره‌مندی آن از امنیت است. دولت‌ها معمولاً موهبت امنیت را بر اصل قدرت اجبار مدیریت جامعه ترجیح می‌دهند؛ چرا که سنگ‌بنای قوام هر تمدن و قوم، تداوم و پایداری سیاسی در مقوله امنیت داخلی است. اکنون امنیت داخلی، در بعدشناسی امنیت، به دنبال یافتن جایگاه و رتبه اعتباری برای خود می‌باشد. اساساً مطالعات امنیتی معاصر، به مباحث امنیت داخلی مانند امنیت ملی توجه نکرده‌اند.

به طور کلی تعاریف ارائه شده در مورد امنیت داخلی را می‌توان به دو رویکرد سلبی و ایجابی تقسیم نمود. در تعاریف ارائه شده بر اساس رویکرد سلبی؛ مفهوم امنیت داخلی بر حفظ توانمندی و شئون‌های دولت و مقابله با جرائم و آسیب‌های سیاسی و نیز توان برقراری نظم و قانون تأکید می‌ورزد. در این رویکرد، رشد جرائم و آسیب‌های سیاسی، موجب به خطر افتادن امنیت داخلی و حمایت دولت می‌گردد و دولت تمام تلاشش را باید معطوف به مصون ماندن از این خطرها نماید.

اما در رویکرد ایجابی؛ امنیت داخلی، شرایطی است که منافع، مصالح و حقوق دولت و نهادهای وابسته به او تأمین می‌شود. در این رویکرد، امنیت داخلی دارای وجوه مختلفی است که عبارتند از: سیاسی، اقتصادی، قضایی، فرهنگی و اجتماعی دولت که منشأ بروز تهدید: «درون واحد ملی»، حوزه تحلیل: «محیط ملی» و واحد تحلیل: «احزاب، گروه‌ها و

نیروهای مؤثر اجتماعی» هستند. در این دیدگاه، از نظر نگرش اطلاعاتی و امنیتی و با هدف ثبات و اقتدار نظام سیاسی، محور تحلیل؛ منافع، مصالح و یا آسیب‌ها و بحران‌های ناشی از عدم ثبات و انتظام ملی است و نیروهای ضد اطلاعات و امنیتی و انتظامی، عهده‌دار حفظ و حراست آن هستند.

در واقع، امنیت داخلی، بستر و زمینه‌ساز ظهور امنیت ملی است. بنابراین، امنیت داخلی با توجه به تعاریف مختلف که از آن ارائه شد، در جامعه براساس تنظیم مناسبات زیر ارائه می‌شود:

- تنظیم مناسبات حقوقی مردم و دولت؛
- تنظیم مناسبات دولت با نهادهای اجتماعی؛
- تنظیم مناسبات بین نهادهای دولت.

همان‌طور که مشاهده می‌شود «دولت و حکومت»، رکن ثابت هر سه وجه امنیت داخلی به‌شمار می‌آیند. به همین دلیل، تلاش برای جلب توسعه نظم عمومی و تمکین سیاسی – اجتماعی مردم، به صورت مستقیم و غیرمستقیم، در دستور کار دولتمردان قرار دارد. بنابراین، می‌توان «امنیت داخلی» را از جهت «کار ویژه» چنین تعریف کرد: «وضعیتی که در آن نظم اجتماعی و سیاسی بین مردم و نهاد دولت از ظهور، توسعه و نهادینه شدن فسادهای مختلف صیانت شده است و در نتیجه شاهد کاهش ضریب ناامنی دولت از ناحیه عملکرد سایر بازیگران محیط می‌باشیم» (بلندیان، ۱۳۸۸: ۵۷).

یا در تعریفی دیگر، امنیت داخلی عبارت است از: «امنیت یک کشور در برابر تهدیدهای آشکار و پنهان درون مرزهای ملی» (خاکسار، ۱۳۸۸: ۲۷).

مفهوم امنیت داخلی از دیدگاه اسلام:

مقوله امنیت و امنیت داخلی، از جمله موضوعات مهم و حساس حکومت است که می‌تواند آینه تمام‌نمای نظریه اقتدار و کارایی آن باشد. اسلام در این زمینه، نظر و عمل بنایی برافراشته است که تا ابدیت پایایی و روایی دارد.

امنیت در اسلام به عنوان یکی از ضروری‌ترین و ابتدایی‌ترین نیازمندی‌های انسان و غایتی ارزشمند برای زندگی فردی و اجتماعی او به حساب می‌آید. توجه به انسان به عنوان شالوده و اساس در مقوله امنیت در بعد فردی و جمعی، کرامت و گرانمایگی او، مشروعیت و مقبولیت مدیر امنیتی، تربیت و تزکیه، صلح‌خواهی و صلح‌سازی و تقدم ابزار نرم برابر سخت در تأمین امنیت داخلی، تقدم و اولویت عدالت بر امنیت، شرعی بودن ابزار تأمین امنیت، قانون‌محوری و...، از جلوه‌های نظریه امنیت دینی است (هاشمیان‌فرد، ۱۳۸۸: ۲۵).

نگاه اسلام به مفهوم امنیت داخلی، نگاه جامع، رو به جلو، ریشه‌ای و همیشگی است. امنیت به عنوان پدیده‌ای جوشنده از درون جامعه، از منظر اسلام، کمال بلوغ را تجربه کرده و دارای تأثیر متقابل از عوامل و پدیده‌های دیگر است. سهیم و شریک دانستن مردم به عنوان تولیدکننده و مصرف‌کننده امنیت، از نعمات بی‌نظیر اسلام است و تأمین امنیت داخلی و برخورداری دولت از نعمت ثبات، جزء وظایف اولیه و مهم حکومت‌ها در مقابل حقوق نمایندگی و مسئولیت و رسالت خود برای اجرای حقوق حکومتی آنها محسوب می‌شود.

امنیت داخلی در تعامل حکومت و جامعه و در دو سطح عینی و ذهنی تجلی می‌یابد.

شاخص امنیت داخلی، به حوزه‌های استقلال سرزمین اسلام و توان توسعه ایدئولوژیک بر می‌گردد.

حضرت علی(ع) نیز امنیت را گواراترین نعمت توصیف نموده و در خطبه ۱۳۱ نهج‌البلاغه، هدف اصلی مبارزه اولیای دین که خود سید ایشان است را برقراری امنیت داخلی ذکر می‌کند و چنین می‌فرماید: «پروردگارا! تو می‌دانی که آنچه ما انجام داده‌ایم، نه برای این است که حکومتی به دست آوریم و نه برای این است که از مقام پست دنیا چیزی فراهم نماییم، بلکه به این خاطر است که نشانه‌های از بین رفته دین تو را بازگردانیم و اصلاح را در شهرهای تو آشکار نماییم تا بندگان ستمدیده تو در امنیت قرار گیرند». در واقع حضرت، فلسفه تشکیل هر حکومتی را تأمین امنیت برای مردم و حقوق الهی می‌داند.

راهبرد حضرت علی(ع) در مقوله امنیت داخلی، در عین توجه به اهمیت بعد سخت‌افزاری، بیشتر رویکردی نرم‌افزارانه دیده می‌شود. به ترتیبی که نقش مردم به عنوان تولیدکننده و مصرف‌کننده اصلی کارهای امنیت، در این رویکرد بی‌بدیل است.

با توجه به مطالبی که بیان شد، می‌توان هدف‌های امنیت داخلی را به‌شرح زیر برشمرد:

۱. ایجاد آرامش و نظم سیاسی؛
۲. تثبیت حاکمیت قانون و مقررات وضع شده در جامعه؛
۳. حفظ انسجام و روابط دولت با مردم؛
۴. تضمین منافع نمایندگی مشروع دولت (همان، ۵۴).

امنیت داخلی، بخشی از امنیت ملی را شامل می‌شود که کارویژه ملی قدرت در دولت است. حفظ مصالح و نظم سیاسی از طریق؛ تنظیم مناسبات و روابط سالم بین جامعه و نهادهای مدنی و بروکراسی تأمین می‌گردد.

پیشگیری از بحران‌های سیاسی – اجتماعی و جبران آثار آن، بر عهده امنیت داخلی است.

امنیت داخلی از یک سو؛ ناظر بر عملکرد سازمان قدرت در کنترل تحولات اجتماعی است و از سوی دیگر؛ عهده‌دار مدیریت مناسبات قدرت میان دولت و مردم و برخورد با عوامل مخل است. امنیت داخلی بر پایه نظارت سامانه‌های امنیتی، بر بازیگران مختلف در جامعه و شبکه روابط قدرت شکل می‌گیرد تا به توانمندی نمایندگی و اقتدار دولت تعرض نشود و اطمینان‌خاطر در دولت ایجاد شود.

۵/ب. تأثیر فناوری بر امنیت داخلی:

تأمین امنیت داخلی و طراحی و هدایت محیط‌های امنیتی و مقابله با تهدیدهای امنیت داخلی، بدون استفاده از فناوری و تکنولوژی‌های مورد نیاز، ممکن نیست. پیشرفت فوق‌العاده و غیرقابل تصور فناوری اطلاعات و ارتباطات سازمان‌های مدنی، تأمین امنیت

را با شرایط و رویارویی‌های واقعی و بسیار جدی روبه‌رو کرده است. امروزه روش‌های برقراری ارتباط و کسب اطلاعات، می‌بایست با شرایط جدید در حوزه فناوری اطلاعات و ارتباطات مطابق باشند، در غیر این صورت اوضاع برای سازمان‌هایی که به‌روز نمی‌باشند، وخیم‌تر خواهد شد (treverton,۲۰۰۲).

فناوری‌های جدید که در جامعه حادث می‌شوند، تأثیر دوگانه‌ای بر امنیت دارند. از سویی؛ موجب تقویت توان اطلاعاتی و انجام وظایف سازمان‌های متولی امنیت می‌گردند و از طرفی؛ خلق آسیب‌ها و تهدیدهای جدید علیه امنیت داخلی جامعه را به ارمغان می‌آورند.

اگرچه فناوری‌های نوین در عرصه اطلاعات و ارتباطات ممکن است تبعات تهدیدآمیز علیه امنیت داخلی داشته باشد، اما برتری امنیتی و اشراف نسبت به فضای اطلاعات و ارتباطات، لازمه تأمین امنیت می‌باشد. فناوری‌های نوین در عرصه اطلاعات و ارتباطات، موجب می‌شود که متولیان و سیاستگذاران امنیت جامعه بتوانند با دستیابی به برتری اطلاعاتی[۱] قدرت پیش‌بینی پدیده‌های اجتماعی را افزایش داده و بنابراین، در تحقق امنیت و پایداری و مقابله با تهدیدهای اجتماعی، از قدرت قابل توجهی برخوردار گردند.

امروزه فناوری به تعبیر الوین تافلر[۲] «آسمان را پر از چشم و گوش کرده است»، که به طور هوشمند داده‌های انبوهی اعم از نظامی، سیاسی، اقتصادی، اجتماعی را جمع‌آوری می‌کنند. ماهواره‌ها و دیگر ابزارهای تصویری، ایستگاه‌های استراق‌سمع و رادارهای غول‌پیکر و دیگر ابزارهای الکترونیکی، تمام نقاط جهان را زیر نظر داشتند و به دلیل همین پیشرفت‌ها، به بخش عمده‌ای از تحرکات و جابه‌جایی افراد و وسایل در سطح کره زمین نظارت می‌کنند (تافلر، ۱۳۷۰: ۵۰۷).

---

۱ . intelligence superiority

۲ . Alvin Toffler

تافلر معتقد است در عصر اطلاعات، دولت‌هایی که از فناوری‌های نوین بیشترین استفاده را می‌کنند، از قدرت بیشتری در راه‌های رسیدن به هدف‌های خود برخوردار می‌باشند. از این‌رو، با توجه به اینکه یکی از هدف‌های مهم همه دولت‌ها، ایجاد امنیت در داخل و خارج خود می‌باشد، مسلماً فناوری اطلاعات و ارتباطات می‌تواند این هدف را برای دولت‌ها تهیه و محقق نماید. از سوی دیگر؛ با استفاده از فناوری‌های نوین، فعالیت‌های ضدامنیتی حریف (چه در داخل و چه در خارج)، قابل شناسایی و ردیابی می‌شود.

فناوری و شناخت امنیت داخلی:

شناخت امنیت داخلی، از مؤلفه‌های مهم تأمین امنیت می‌باشد. احصاء فرصت‌ها و تهدیدها و شناسایی نقاط قوت و ضعف عوامل ناامنی و به عبارت دیگر؛ اشراف امنیتی مناسب، حاصل این شناخت می‌باشد. برای رسیدن به شناخت، ضرورت نظارت بر فعالیت‌های مخل امنیت داخلی، امری ناگزیر است و باید به صورت آگاهانه نسبت به این امر اقدام نمود.

برای رسیدن به نظارت مطلوب، لازم است وظیفه جمع‌آوری اخبار و اطلاعات در سازمان‌های متولی امنیت داخلی به نحو مطلوب انجام پذیرد. جمع‌آوری اطلاعات، مأموریت اصلی هر سازمان امنیتی است که هدف از آن کسب اطلاع از هدف یا حریف، به منظور نظارت و کنترل بر فعالیت‌های اجتماعی ضدامنیتی و آگاهی از مقررات، ضعف‌ها و توانمندی‌های عوامل ضدامنیتی می‌باشند.

هر اندازه سازمان‌های متولی تأمین امنیت داخلی، از اشراف و نظارت بیشتری نسبت به پیرامون خود برخوردار باشند، به همان میزان قدرت پیشگیری نیز در اختیار خواهند داشت. سطح نظارت امنیتی، به میزان شناخت از محیط امنیتی بستگی دارد.

«گری مارکس» نظارت را استفاده از ابزارهای فنی برای بررسی افراد یا موقعیت‌ها برای استخراج یا ایجاد داده‌های مشخص می‌داند. او پنج بُعد از جنبه‌های نظارتی در سازمان‌های امنیتی را به شرح زیر عنوان می‌کند:

- ساختارهای محیطی که نظارت در آنها مورد استفاده قرار می‌گیرد؛
- ویژگی‌های ابزاری که در نظارت به کار گرفته می‌شوند؛
- محتوا و نوع داده‌هایی که جمع‌آوری می‌شوند؛
- به کارگیری ابزار از جمله جمع‌آوری داده‌ها و تحلیل و بررسی آنها؛
- هدف‌هایی که در فرآیند نظارت دنبال می‌شود (marx,۲۰۰٤,p.p۲۲٤-۲٤۹).

با این توضیحات، نظارت امنیتی در این معنا، به مفهوم امکان اشراف و رصد موضوعات امنیتی در محیط ملی و پیرامونی و نیز شناسایی آسیب‌ها و تهدیدهای امنیتی به منظور طراحی شیوه‌های مناسب مقابله با آن می‌باشد. بدون نظارت مطلوب بر عوامل مؤثر در امنیت داخلی، نمی‌توان در تحقیق امنیت و ثبات موفق باشیم.

از مهم‌ترین عوامل مؤثر در ایجاد امنیت داخلی، می‌توان به موارد زیر اشاره کرد:

- قانون‌محوری، قانون‌گرایی، اجرای دقیق قانون و پایبندی همگان به‌ویژه نهادهای رسمی قدرت حاکم به قواعد و مقررات اجتماعی، موجب تقویت پایه‌های امنیت اجتماعی است؛
- اقتدار حکومت همراه با سلامت اخلاقی و تعهدورزی در کنترل جامعه عامل بسیار مؤثر در حفظ و ارتقای امنیت اجتماعی است؛
- تأمین حقوق و آزادی‌های فردی به‌ویژه تعیین حدود و مرزهای حقوق فردی و احترام و پایبندی به آن خصوصاً از جانب نهادهای رسمی، عامل دیگر در تقویت امنیت داخلی است؛
- فضاسازی برای مشارکت تمام مردم و شهروندان در عرصه‌های متفاوت اجتماعی، سیاسی، فرهنگی، اقتصادی، مذهبی؛

- توجه به کرامت انسان، گرانمایگی اخلاق و صفات اخلاقی به عنوان یک «ارزش‌های تعلیم یافته»، برای جلوگیری از فروپاشی نظام اخلاقی و کاهش ارزش انسان‌ها از مقوم‌های امنیت داخلی است؛
- اعتماد ملی، خوش‌بینی و غلبه بر بدبینی در شکل عام آن که «اعتماد تعلیم‌یافته» را گسترش می‌دهد، عامل مؤثر در تأمین امنیت داخلی به‌شمار می‌آید؛
- گسترش و تعمیم دایره سرمایه‌های امنیت در جامعه نیز موجب حفظ، گسترش و ارتقای سطح و کیفیت امنیت داخلی است؛
- افزایش دامنه تعاملات، ارتباطات، همکاری متقابل اعضای جامعه و دولت با یکدیگر، پیوستگی ارتباط اعتمادزا، تعهدآفرین و حمایت‌کننده در جامعه را که همانا تقویت امنیت داخلی است، به دنبال دارد؛
- توسعه روابط با سایر جوامع دینی و افزایش اعتبار و موقعیت بین‌المللی، کمک مؤثری در حل چالش‌های سطح بین‌الملل دارد و همین موجب تقویت انسجام ملی و امنیت داخلی در جامعه اسلامی می‌شود (بلندیان، ۱۳۸۸: ۲۸-۲۷).

مهم‌ترین تأثیرهای فناوری بر نظارت و شناخت امنیتی، عبارتند از:

- ارتقاء روش‌های جمع‌آوری اطلاعات اعم از آشکار، انسانی، فنی؛
- افزایش تولید اطلاعات راهبردی؛
- افزایش شناخت نسبت به توان تأثیر پدیده‌ها؛
- توانایی و تسریع در اتخاذ اقدام مناسب؛
- شناسایی و تعیین دقیق فرصت‌ها، قوت‌ها، آسیب‌ها و تهدیدهای امنیتی در جامعه؛
- پیشگیری از غافلگیری امنیتی؛
- کسب مهارت‌های دقیق و هوشمند در مواجهه با ناامنی‌های اجتماعی.

فناوری و کنترل امنیت داخلی:

کنترل امنیت داخلی، از جمله هدف‌های مهم سازمان‌های امنیتی کشور می‌باشد که «فناوری» نقش بسیار مهمی در رسیدن به این هدف دارد. مقابله با پدیده‌های ضدامنیتی جامعه نظیر؛ جریان‌سازی، انشعاب، کودتا، ترور، خرابکاری و مانند آن، در صورتی به خوبی انجام می‌شود که بتوان این پدیده ضدامنیتی را کنترل و خنثی نمود. در این میان، فناوری نقش بسیار مهمی را ایفا می‌کند.

فناوری موجب شده تا روند شناخت تهدیدهای امنیت داخلی و مقابله با آنها، از نگاه سنتی تغییر چهره داده و با رویکردهای جدیدی مواجه شوند. ریشه فناوری، تجدید ساختار روابط درونی شبکه‌ها، ایجاد شبکه‌های جدید در اجتماع و برقراری نوع نوینی از ارتباطات، موجب شده سازمان‌های متولی امنیت کشور در برابر تغییرات اساسی قرار بگیرند. چنانچه به تعبیر شولسکی، اطلاعات را اخبار موثقی بدانیم که با تدوین و اجرای سیاست کشورها برای تأمین منافع امنیتی و مقابله با تهدیدهای حریفان بالفعل یا بالقوه نسبت به آن منافع سروکار دارد (shulsky,۱۹۹۳,۱۲)، می‌توان فناوری را در تمام حوزه‌های اطلاعاتی از جمله کنترل، دخیل دانست.

فناوری‌های نوین، در قالب زیرساخت‌های حیاتی و ابزارهای کاربردی به عنوان عوامل اعمال اثر قدرت مورد استفاده قرار می‌گیرند و هدف‌های امنیتی در محیط حریف تعقیب می‌شوند. ارتقاء قدرت از طریق نرم‌افزاری توسط فناوری‌های نو، موجب می‌شود توانایی کسب منابع مطلوب برای سرویس امنیتی خود فراهم شود.

فناوری همچنین قادر است محیط غیرقابل دسترس را به محیط قابل کنترل برای سرویس‌های تأمین امنیت تبدیل نماید. ارتقای قدرت از طریق نرم‌افزاری توسط فناوری‌های نو موجب می‌شود توانایی کسب نتایج مطلوب در تأمین امنیت داخلی فراهم شود. توانایی به دست آوردن نتایج مطلوب از طریق جلب نظر دیگران و نه مجبور کردن آنها که با متقاعد کردن دیگران به پیروی و یا واداشتن آنها به قبول هنجارها و نمادهایی که رفتار مطلوب را به وجود می‌آورند، موجب اعمال قدرت و به عبارتی؛ کنترل محیط

امنیتی می‌شود. این نوع قدرت به تعبیر جوزف نای می‌تواند جذابیت اندیشه‌ها یا فرهنگ فرد یا توانایی تعیین دستور کار از طریق معیارها و نهادهایی باشد که موجب تغییر در ترجیحات دیگران می‌شود (نای و کیئن، ۱۳۹۰: ۳۶۸).

فناوری موجب می‌شود که دولت بتواند قدرت خود را به صورت مسالمت‌آمیز اعمال نماید و در چنین شرایطی میزان کنترل بر تصمیمات، نیات و هدف‌های دیگران افزایش می‌یابد. بنا به تعبیر «مایکل هرمن» پیشرفت‌های فناوری، مرزها را از میان برداشته و به ویژه مرزهای جغرافیایی را تیره و تار کرده و بر کنترل ملی مرزها اثر می‌گذارد (Herman,۱۹۹٦,٥۲).

فاصله بین بازیگران دولتی و غیردولتی در دستیابی به فناوری‌های پیشرفته، زیادتر شده و به همین نسبت، میزان کنترل امنیت اجتماعی توسط بازیگران دولتی افزایش یافته است.

اگرچه در عرصه جمع‌آوری و تحلیل امنیتی، بازیگران متعددی وارد عرصه شده‌اند، اما توانایی آنها به میزان قدرت بازیگران دولتی نیست و نمی‌توانند همان نقش‌ها را برعهده گیرند. فناوری به عنوان مؤلفه‌ای تأثیرگذار بر تحول کنترل محیط امنیت داخلی در پویش کنشگران دولتی، موجب شده تا حوزه عمل کنترل امنیت داخلی به لحاظ عمل و اجرا در واقع فرا مکانی، پُرشتاب، چندمرکز و شبکه‌ای شود. با چنین توصیفی، اشراف و کنترل تهدیدهای امنیت داخلی افزایش می‌یابد.

مهم‌ترین تأثیرهای فناوری بر کنترل امنیت داخلی عبارتند از:

- تبدیل محیط غیرقابل کنترل، به محیط قابل دسترسی و کنترل؛
- حذف مکان و زمان در اجرای تدابیر امنیتی؛
- شناسایی سریع‌تر، بهنگام و آسان‌تر تهدیدهای امنیت داخلی؛
- مساعدت در اقدام‌های اجتماعی، سیاسی و فرهنگی مطلوب؛
- تغییر پارادایم کنترل امنیتی سلبی، به ایجابی و هوشمند؛
- امکان کنترل و پایش افکار عمومی؛
- گسترش کمیت و کیفیت منابع و ابزارهای امنیتی؛

- کنترل خبر و اطلاعات از پدیده‌های اجتماعی و امنیتی.

شاخص‌های فناوری در امنیت داخلی جمهوری اسلامی ایران:

تحقق هدف‌های نظام و چشم‌انداز بیست ساله، بدون پرداختن به فناوری اطلاعات و ارتباطات، در سه بعد مختلف ممکن نیست. این سه بعد عبارتند از:

- توسعه فناوری اطلاعات و ارتباطات و تحقق خوداتکایی در حد ضرورت؛
- توسعه کاربری فناوری اطلاعات و ارتباطات؛
- توسعه مدیریت فناوری اطلاعات و ارتباطات.

لازمه موفقیت، حرکت متوازن و متناسب هر سه محور است. هدف اصلی کشور، توسعه همه‌جانبه، هوشمندانه، و اثربخش کاربری فناوری اطلاعات و ارتباطات و حداکثر بهره‌برداری از فرصت‌های نهفته در این فناوری است؛ و لازمه تحقق این هدف، زمینه‌سازی‌های کافی و به‌موقع در دو محور دیگر است. رشد فناوری در سال‌های اخیر، علاوه بر تأثیرگذاری در حوزه‌های سیاسی، اقتصادی و اجتماعی، موجب شده در حوزه امنیتی خصوصاً امنیت داخلی، فعالیت‌های امنیتی را تحت تأثیر قرار دهد.

گرایش‌های رفتاری، زیر بنای نهفته در انقلاب تکنولوژی به تعبیر برکوویز شامل افزایش توانمندی‌ها، کاهش هزینه‌ها و ارتباطات سریع می‌شود (Berkowiz and Goodman,۲۰۰۰,۳۶).

این سه مؤلفه، در حوزه نظارت و کنترل اطلاعاتی نیز موجب شده شاخص‌های تأمین امنیت داخلی تحت‌تأثیر نیازمندی‌های سایت اطلاعاتی قرار گیرند. عوامل تأمین امنیت داخلی، ترکیبی از توانایی و نظارت امنیتی و تقویت کنترل امنیتی می‌باشند که فناوری به شدت با این حوزه‌ها ترکیب می‌یابد. هرچه یک سازمان متولی امنیت، از فناوری و تکنولوژی مدرن‌تری در نظارت و کنترل اطلاعاتی برخوردار باشد، به همان میزان در اشراف امنیتی به حریفان، موفق‌تر خواهد بود.

در این مقاله با برگرفتن از نظرهای کارشناسی تعدادی از خبرگان حوزه فناوری و امنیت که از مدیران ناجا و اساتید دانشگاه می‌باشند، شاخص‌های فناوری اطلاعات و

ارتباطات در امنیت داخلی جمهوری اسلامی ایران که نقش مهمی در تأمین امنیت داخلی دارند، عبارتند از:

۱. ارتقاء روش‌های جمع‌آوری اطلاعات:

توانایی جمع‌آوری، کنترل و بهره‌برداری اطلاعات، موجب برتری اطلاعاتی می‌شود.

فناوری اطلاعات و ارتباطات، بستری برای جمع‌آوری اطلاعات می‌باشد.

امنیت، فرآیندی است جهت مقابله با تهدید علیه ارزش‌های حیاتی یک جامعه.

مفهوم امنیت، به دو متغیر اصلی تهدید و ارزش‌های ملی وابسته است.

اطلاعات به عنوان یک سلاح نرم، قادر است به گونه‌ای تدریجی سبب بروز تغییرات در منافع، تعریف منفعت و شاخص‌های مهم منفعت گردد.

اطلاعات به عنوان یک عامل پوشیده، اما توانمند، قادر است تأثیرهای قابل توجهی را بر ارزش‌های حیاتی یک جامعه بگذارد.

تأثیرهای موردنظر یعنی همان تغییر ارزش‌های حیاتی به واسطه اطلاعات جدید را در یک حالت می‌توان تهدید قلمداد نمود و در حالتی دیگر می‌توان آن را صرفاً یک تغییر مبنی بر تکامل محسوب نمود (فناوری و قدرت ملی، ۱۳۸۸: ۳۱۰).

۲. افزایش کیفیت و دقت در شناخت تهدید:

تهدید، از سه بخش اساسی؛ «عامل تهدید»، «حوزه تهدید» و «موضوع تهدید» تشکیل شده است. عامل تهدید، در واقع هویت (شخصی یا سازمانی) یا چیزی است که به طور بالفعل و بالقوه توانایی ایجاد، انفعال یا پشتیبانی از تهدید را دارد. در حالی که حوزه تهدید، هویت یا چیزی است که موجودیت و یا دارایی‌های حیاتی آن در معرفی خطر قرار گرفته است. موضوع تهدید، وضعیت، پدیده، فعالیت، یا رخدادی است که به نظر می‌رسد قابلیت‌های درونی و بیرونی انتقال، پشتیبانی یا ایجاد خطر در موجودیت یا دارایی‌های حیاتی بازیگر مورد آماج را در خود دارد (عبدالله‌خانی، ۱۳۸۶: ۲۱).

فناوری سبب گردیده که برداشت از تهدید، در مبادلات امنیتی تغییر نماید و جلوه تهدیدهای امنیتی در نزد تحلیلگران امنیتی، با کیفیت و دقت بیشتری شناسایی و قابل کنترل شود.

فناوری اطلاعات با ایجاد دگرگونی در فهم از منفعت که از تغییر آگاهی، فهم و دانش ناشی می‌گردد، به نوبه خود سبب شکل‌گیری و تکامل جدیدی از ارزش‌های حیاتی و باورهای بنیاد می‌گردد (فناوری و قدرت ملی، ۱۳۸۸: ۳۳۹).

۳. افزایش تولید اطلاعات راهبردی:

یکی از برجسته‌ترین شیوه‌های کسب برتری اطلاعاتی، تولید اطلاعات راهبردی است. در واقع با تولید اطلاعات راهبردی، قوای قدرت ملی در راستای تقویت اطلاعاتی بر حریف، بسیج می‌گردد. «شلتون» یکی از مفسرین سند دکترین عملیات اطلاعاتی پنتاگون، در خصوص تولید اطلاعات راهبردی چنین می‌گوید: «عملیات اطلاعاتی در سطح راهبردی، تحت امر فرماندهی ملی، به منظور دستیابی به هدف‌های ملی، از طریق اثرگذاری بر تمامی عناصر قدرت ملی دشمن (سیاسی، نظامی، اقتصادی، اطلاعاتی و غیره) و هم‌زمان دفاع از تمامی عناصر قدرت ملی صورت می‌گیرد. هماهنگی میان نیروهای نظامی بخش‌های مختلف دولت امریکا و هم‌پیمانان کشور جهت اجرای چنین عملیاتی، در بالاترین سطح ممکن قرار دارد».

اگرچه این تعریف در خصوص امنیت ملی امریکا ارائه شده و بیشتر منظور آن تهدیدهای خارجی امنیت ملی می‌باشد، اما ملاحظه می‌شود که توان اطلاعاتی راهبردی چقدر در بررسی اطلاعاتی تأثیرگذار است. بنابراین، در امنیت داخلی نیز سازمان‌های متولی امنیت، بایستی از توان اطلاعاتی راهبردی قابل قبول برخوردار باشند و بتوانند بر تهدیدهای امنیت داخلی غلبه نمایند.

فناوری اطلاعات و ارتباطات، نقش بسیار کلیدی در افزایش تولید اطلاعات راهبردی دارد. در ورای شکل‌گیری رقابت در حوزه اطلاعات (که به عنوان امری طبیعی قلمداد می‌گردد)، حوزه اطلاعات به عنوان اصلی‌ترین سازنده و در حقیقت سنگ‌بنای قدرت نرم

کشورها، از یک کاربری سیاسی به منظور نیل به هدف‌های سیاسی و امنیتی برخوردار می‌گردد (همان، ۳۴۵).

افزایش تولید اطلاعات راهبردی به منظور تأمین امنیت پایدار، موجب اشراف اطلاعاتی و عملکرد راهبردی صحیح می‌شود و فناوری اطلاعات و ارتباطات، از جمله عوامل اصلی و مهم در تولید اطلاعات راهبردی می‌باشد.

۴. افزایش شناخت نسبت به تأثیر پدیده‌ها:

ویژگی‌ها و ماهیت امنیت داخلی معمولاً سبب بروز رخدادها می‌گردد که از این رخدادها به نام پدیده یاد می‌کنیم. پدیده اثر چندین عامل و متغیر است که رخداد ناشی از وقوع آن، تبعاتی پیچیده و ناشناخته دربر دارد. مطالعه پدیده از چند جنبه حائز اهمیت است: اول؛ اثرها و ویژگی‌های ذاتی پدیده و دوم؛ عوامل و متغیرهای شکل‌گیری یک پدیده. شناخت بیشتر پدیده‌ها، خصوصاً پدیده‌های اجتماعی، ما را در تعیین هدف‌های موردنظر در تأمین امنیت داخلی و همچنین طراحی مکانیزم اجرایی لازم، یاری می‌رساند. چرا که از مطالعه پدیده‌ها پی می‌بریم که اعمال تأثیرهای مختلف بر هدف، چه نتایجی را خواهد داشت و به این ترتیب، امکان طراحی مدل امنیتی مناسب فراهم می‌شود.

۵. ارتقاء توانایی در اتخاذ اقدام هدفمند:

هدف اولیهٔ استفاده از فناوری اطلاعات، «آگاهی» است و درک و برداشت نوین از تهدیدها، امکان اقدام متقابل را برای دفع تهدید فراهم می‌آورد. امنیت به کمک فناوری، از توان اتخاذ اقدام مناسب با تهدید، براساس شناخت دقیق و هدفمند، برخوردار می‌گردد.

۶. تقویت بررسی، تحلیل و ارزیابی:

تأثیر اصلی فناوری اطلاعات، بالابردن حداکثر و سرعت تصمیم‌گیری؛ یعنی سرعت اندیشیدن است. در نتیجه این پیشرفت‌های فناوری، سرعت و قدرت تحلیل و ارزیابی برای درپیش گرفتن اقدامات مختلف در محیط امنیتی را افزایش می‌دهد (روزنا، ۱۳۹۰: ۴۵۰).

۷. شناسایی نقاط قوت، ضعف و تهدید:

از جمله شاخص‌های فناوری اطلاعات، شناسایی نقاط قوت، ضعف و تهدید در امنیت داخلی است که موجب می‌شود دقت در تصمیم‌گیری‌ها و تدوین راهبردهای میان‌مدت و بلندمدت را آسان‌تر و پیش‌بینی‌های مطمئن‌تر ممکن‌تر شود و در نتیجه؛ هزینه‌های امنیتی کاهش یابد.

۸. کسب مهارت‌های هوشمند در مبارزه با تهدیدهای امنیتی:

عوامل ناامنی که باعث بی‌ثباتی در کشور می‌شوند، از تهدیدهای داخلی نشئت می‌گیرند. وجود اقلیت‌های قومی، مذهبی، یا تعدد زبانی و تفاوت‌های فرهنگی در برخی زمینه‌ها، ممکن است فرصت‌هایی را برای بهره‌برداری کشورهای متخاصم، به منظور ایجاد بحران‌های هویتی یا جدایی‌طلبانه ایجاد کند.

مردم و نظام سیاسی، بایستی به مهارت‌های ذهنی و عینی لازم از نظر سیاسی، اجتماعی، فرهنگی رسیده باشند یا بتوانند علی‌رغم قومیت‌ها و اقلیت‌های متعدد، در چارچوب و محدوده مرزی مشخص، در قالب کشوری واحد به طور مسالمت‌آمیزی با هم زندگی نمایند. افکاری نظیر؛ جدایی‌طلبی و ناحیه‌گرایی، اختلافات سیاسی، مذهبی و قومی، می‌بایست تحت‌الشعاع اموری از قبیل؛ پیشرفت‌های علمی، فناوری، رفاه اقتصادی، تأمین عدالت اجتماعی، نهادینه شدن قانون و حقوق فردی و جمعی قرار بگیرد و حاکمیت نیز منافع و ارزش‌های عمومی را در صدر برنامه‌های خود قرار دهد. فناوری هوشمند، می‌تواند مهارت‌های مختلف در مقابله با تهدیدهای امنیتی را در اختیار برنامه‌ریزی امنیتی قرار دهد (غفورزاده و رنو، ۱۳۸۸: ۷۳-۷۲).

شاخص‌هایی مانند؛ مشارکت سیاسی، ثبات سیاسی، استقلال، رشد اقتصادی، توسعه‌یافتگی، رفع فساد و تبعیض‌های ناروا، دانش‌اندوزی و رفع بی‌سوادی، سلامت جسمی و روحی انسان‌ها، سلامت محیط زیست بشری و... ارزش‌های متکثر امنیتی را دربر می‌گیرند که فناوری اطلاعات و ارتباطات، نقش بسیار مهمی در شکوفایی این ارزش‌ها در تأمین امنیت داخلی دارد.

۹. شکل‌گیری فضای آزمون‌پذیر و قابل تکرار در تأمین امنیت داخلی:

سازمان‌های امنیتی با کمک فناوری اطلاعات و ارتباطات، می‌توانند محیط غیرقابل دسترس را به محیط قابل کنترل برای تأمین امنیت، تبدیل نمایند و مجموعه قابلیت‌های بالفعل ملی کشور را در راستای منافع ملی شکل داده و تغییرهای دلخواه را در رفتار بازیگران ایجاد نمایند.

شکل‌گیری فضای آزمون‌پذیر و قابل تکرار در تأمین امنیت داخلی توسط فناوری اطلاعات و ارتباطات، می‌بایست قابل تحقق باشد و سازمان‌های امنیتی و متولی امنیت داخلی، بتوانند در فضای آزمون‌پذیر، هدف‌های عملکرد امنیتی خود را مورد بررسی قرار دهند.

۱۰. رشد و توسعه اطلاعات شبکه‌ای:

هدف نهایی فناوری اطلاعات و ارتباطات و ارائه اطلاعات و شناخت دقیق و هدفمند به مشتریان، به گونه‌ای که به آن نیاز دارند، می‌باشد. چنانچه اطلاعات نتواند دارای این مشخصات باشد، به‌طور کلی فاقد نتیجه مطلوب و پایه‌ای خواهد بود و فناوری اطلاعات و ارتباطات در حوزه امنیت داخلی، می‌بایست واجد چنین شاخصی برای مهیا نمودن فضای اطلاعات و ارتباطات شبکه‌ای برای تصمیم‌گیران امنیت باشد. رشد و توسعه اطلاعات شبکه‌ای، اشراف امنیت ملی و همچنین فضای مناسب برای بهره‌مندی از ارتباطات همه‌جانبه برای سازمان‌های امنیتی را مهیا می‌سازد (Brown & Warren,۱۹۹۶,۱۶۵).

امروزه دسترسی به اطلاعات و ارتباطات سریع، درست و همه‌جانبه از جمله لوازم و ابزارهای مورد نیاز تصمیم‌گیران امنیتی کشور می‌باشد که به‌نحوی بعد مکانی یا زمانی، نتواند موجب قضاوت در سطح بهره‌مندی از اطلاعات گردد. مسئولان امنیتی کشور، می‌بایست در هر نقطه از کشور بتوانند به‌راحتی به اطلاعات و ارتباطات مورد نیاز دسترسی داشته باشند و این امر توسط فناوری اطلاعات و ارتباطات محقق می‌گردد.

۱۱. کاهش شکست و غافلگیری‌های امنیتی:

با توجه به پیچیدگی‌های مفهوم تهدید علیه امنیت داخلی، موضوعاتی مانند؛ قدرت، کیفیت زندگی، حاکمیت دولت، هدف‌ها و منافع و ارزش‌های امنیتی یا حیاتی، به عنوان موضوع‌های در معرض تهدید مطرح می‌شوند و بحران‌های امنیتی موجب غافلگیری مسئولان و کاملاً به شکست امنیتی منجر می‌شود. بحران‌ها علاوه بر داشتن شرایط تهدید، از نظر زمانی و مجال تصمیم‌گیری، بسیار محدود هستند. به‌نحوی که عدم تصمیم‌گیری در زمان کوتاه، آثار مطلوب و خشونت‌باری را تولید می‌کند (برچر، ۱۳۸۲: ۲۵).

فناوری اطلاعات و ارتباطات، بایستی این قابلیت را برای مسئولان امنیتی ایجاد کند که بتوانند به‌موقع با رصد تحولات امنیتی و وقایع جامعه، تهدید را شناسایی و از بحرانی شدن امنیت، جلوگیری نمایند.

۱۲. افزایش نفوذ در محیط‌های ضد امنیتی:

در محیط‌های امنیتی، فناوری اطلاعات می‌بایست این قابلیت را داشته باشد که بتواند در محیط‌های ضدامنیتی نفوذ کرده و با استفاده از اطلاعات کسب شده، بتواند مسئولان را در شناخت و کنترل هرچه بهتر تهدید ضدامنیتی، یاری رسانند. در واقع برای مقابله با تهدیدهای امنیت اجتماعی، بایستی تحرکات گوناگون مخالفین نظام، مانند؛ تحریک و تشویق به مبارزات خشونت‌طلبانه یا حتی مسالمت‌آمیز، برپایی انقلاب‌های مخملین و... مورد شناسایی قرار گیرد و فناوری اطلاعات و ارتباطات در امنیت داخلی، باید این قابلیت را داشته باشد که بتواند با نفوذ در محیط‌های ضدامنیتی، اطلاعات راهبردی را در اختیار متولیان امنیت داخلی قرار دهد.

نتیجه‌گیری:

رشد فناوری اطلاعات و ارتباطات در سال‌های اخیر، علاوه بر تأثیرگذاری در حوزه‌های سیاسی، اجتماعی، فرهنگی و اقتصادی، موجب شده است در حوزه امنیتی خصوصاً امنیت داخلی، تأثیرهای عمیق گذاشته و فعالیت‌های امنیتی را تحت‌الشعاع قرار دهد. در این مقاله تلاش نمودیم با تبیین مفهوم فناوری و امنیت داخلی، به تأثیر فناوری

اطلاعات و ارتباطات بر امنیت اشاره و شاخص‌های فناوری اطلاعات و ارتباطات را در امنیت داخلی بیان نماییم.

درک و برداشت نوین از تهدیدها و نیز درک واقعی و حقیقی ارزش‌های حیاتی، موجب شده تا درک کامل‌تر و بهتری از امنیت داخلی صورت پذیرد. همچنین در این مقاله، با بررسی نقش فناوری در شناخت محیط امنیت داخلی و کنترل امنیت داخلی، با بهره‌گیری از نظرهای کارشناسان حوزه امنیت داخلی، اهم شاخص‌های فناوری ارتباطات و اطلاعات را مشخص نماییم. اگرچه مسلماً شاخص‌های دیگری نیز مطرح می‌باشد که ممکن است در این مقاله به آنها اشاره نشده باشد، اما با توجه به محدودیت‌های موجود این تحقیق، اهم شاخص‌های فناوری اطلاعات و اطلاعات که در صفحات قبلی به طور مفصل بیان شد، در قالب جدول زیر مشخص می‌گردد:

جدول ۱: شاخص‌های فناوری اطلاعات و ارتباطات در امنیت داخلی

ردیف	موضوع	حوزه تأثیرگذاری
۱	ارتقاء روش‌های جمع‌آوری اطلاعات	نظارت و شناخت محیط امنیت داخلی
۲	افزایش کیفیت و دقت در شناخت تهدید	نظارت و شناخت محیط امنیت داخلی
۳	افزایش تولید اطلاعات راهبردی	نظارت و شناخت محیط امنیت داخلی
۴	افزایش شناخت نسبت به تأثیر پدیده‌ها	کنترل محیط امنیت داخلی
۵	ارتقاء توانایی در اتخاذ اقدام هدفمند	کنترل محیط امنیت داخلی
۶	تقویت بررسی، تحلیل و ارزیابی امنیتی	نظارت و شناخت محیط امنیت داخلی
۷	شناسایی نقاط قوت، ضعف و تهدید	نظارت و شناخت محیط امنیت داخلی
۸	کسب مهارت‌های هوشمند در مبارزه با تهدیدهای امنیتی	کنترل محیط امنیت داخلی
۹	شکل‌گیری فضای آزمون‌پذیر و قابل‌تکرار در تأمین امنیت داخلی	کنترل محیط امنیت داخلی
۱۰	رشد و توسعه اطلاعات شبکه‌ای	شناخت و کنترل محیط امنیت داخلی
۱۱	کاهش شکست و غافلگیری‌های امنیتی	کنترل محیط امنیت داخلی
۱۲	افزایش نفوذ در محیط‌های ضد امنیتی	کنترل محیط امنیت داخلی

رشد فناوری با شتابی که در پیش دارد، نشان می‌دهد که سطح تأثیرهای این پدیده بر فعالیت‌های سازمان‌های امنیتی، در حال فزونی است و در آینده، تمام حوزه‌های امنیتی را دربر می‌گیرد. طبعاً سازمان‌هایی که خواهان حضور در عرصه رقابت با سایرین هستند، لاجرم به دلیل ضرورت تأمین امنیت محیط ملی خود، نیازمند به‌کارگیری مناسب فناوری در سازمان هستند. فناوری باعث شده که فعالیت‌های تأمین امنیت با سرعت بالا، انطباق‌پذیری فوق‌العاده و چابکی بسیار انجام شود (Metz,۲۰۰۰: ۹).

در دوره‌ای از تاریخ، مفهوم امنیت داخلی عمدتاً شکل سرکوب و خفقان بود؛ یعنی جامعه‌ای امن محسوب می‌شد که قدرت حاکمیت توانایی سرکوب مخالفان و منتقدان را داشت و کسی جرئت ابراز وجود در قبال حاکمیت را نداشت. در واقع شکل سلبی امنیت داخلی، آن هم به معنی سرکوب و دفع تهدید مطرح بود و این موارد از مشخصه‌های برقراری امنیت به‌شمار می‌آمدند و اگر حاکمیتی از قدرت نظامی و امنیتی کمتری برخوردار بود، قادر به تأمین امنیت نبود. اما امروزه عملاً ایجاد امنیت در شکل ایجابی آن مطرح است و نهادهای مدنی و مشارکت مردم، نقش بسیار مهم و کلیدی در امنیت داخلی دارد.

امروزه رشد فناوری و تکنولوژی پیشرفته در صنایع هسته‌ای، نظامی، فضایی و مانند آن، منجر به شکل‌گیری جامعه اطلاعاتی قدرت‌مدار گردید. فناوری همچنین موجب تغییر سیستم می‌شود. شاخص‌های جدید فناوری خصوصاً در بعد اطلاعات و ارتباطات که مهم‌ترین آن در این مقاله به آن اشاره شده است، در میزان قدرت کشورها محاسبه می‌گردد.

فناوری موجب تغییر در نظم سلسله‌مراتبی که مدت‌ها مبنای میزان اعمال اقتدار، فرماندهی و کنترل بود، گردیده است. این تغییر موجب شده تا نظام‌های پیشین، محدود و ضعیف گشته و به جای آن، شکل‌های بدیل شبکه‌محور جایگزین شوند. گسترش فناوری، بسیاری از قلمروهای امنیتی از جمله نظارت و کنترل را درنوردیده و فعالیت‌های جامعه اطلاعاتی را دگرگون کرده است. هرچه فناوری توسعه‌یافته‌تر شده است، بر

شتاب، شدت، گستره و عمق تأثیرگذاری آن بر امنیت داخلی افزوده شده است. در کنار این مزیت، نباید از تهدید فناوری در حوزه عملکرد سازمان امنیتی نیز غافل شد. ظهور بازیگران ضدامنیتی و دسترسی آنها به فناوری و حوزه‌هایی که قبلاً فقط در دسترس سازمان‌های امنیتی بود، از جمله این تهدیدهاست. پیشرفت‌های فناوری، موجب شده تهدیدهای امنیتی، شکل بدیع‌تری پیدا کرده و مقابله با آنها نیز از جهتی مشکل‌تر و پیچیده‌تر شده است.

تحمیل هزینه‌های گزاف بر سازمان‌های امنیتی، از دیگر پیامدهای رشد فناوری است. رقابت در عرصه فناوری میان سازمان‌های امنیتی و حریفان، بسیار گسترده، پر هزینه و پیشرفته‌تر شده است. ضمن اینکه نباید از افشای اطلاعات طبقه‌بندی شده که به دلیل پیشرفت فناوری صورت می‌گیرد، غافل ماند؛ این امر موجب گردیده که سطح دسترسی افراد و بازیگران فاقد صلاحیت، به اخبار و اطلاعات طبقه‌بندی شده، افزایش یابد

در پایان، بایستی اذعان نمود که رشد و پیشرفت فناوری اطلاعات و ارتباطات، موجب تحول در عرصه امنیت داخلی گردیده است. در صورت ایجاد یک امنیت پایدار و باثبات، بایستی شاخص‌های فناوری اطلاعات و ارتباطات در امنیت داخلی، به شرحی که در این مقاله ذکر گردید، لحاظ شود.

تغییر روندهای سیاسی، به ترتیبی است که قدرت نرم‌افزاری نسبت به قدرت سخت‌افزاری در مقایسه با گذشته، اهمیت بیشتری پیدا می‌کند (نای، ۱۳۹۰: ۳۷۸).

منابع:

- بلندیان، غلامحسین (۱۳۸۸)، «**جامعه‌شناسی امنیت داخلی**»، تهران: داعا.
- بوزان، باری (۱۳۷۷)، «**انقلاب و تکنولوژی نظامی**»، ترجمه محب‌علی دیانی، دانشگاه امام حسین(ع)، پژوهشکده علوم دفاعی، تهران.
- تافلر، الوین (۱۳۷۰)، «**جابجایی در قدرت**»، ترجمه شهیندخت خوارزمی، تهران: نو.
- توکل، محمد (۱۳۹۰)، «**جامعه‌شناسی تکنولوژی**»، تهران: نشر جامعه‌شناسان.
- دانشگاه عالی دفاع ملی (۱۳۸۸)، «**فناوری و قدرت ملی (چالش‌ها و راهبردها)**»، تهران: داعا.
- دانشگاه عالی دفاع ملی (۱۳۸۸)، «**نقش فناوری در پویاسازی مدیریت راهبردی**»، تهران: داعا.
- زرقانی، سیدهادی (۱۳۸۸)، «**مقدمه‌ای بر قدرت ملی: مبانی، کارکردها، محاسبه و سنجش**»، تهران: پژوهشکده مطالعات راهبردی.
- سلمان خاکسار، عبدالحمید (۱۳۸۸)، «**حکومت، فرد و امنیت**»، تهران: داعا.
- عبدالله‌خانی، علی (۱۳۸۳)، «**نظریه‌های امنیت: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی**»، مؤسسه ابرار معاصر، تهران.
- غفورزاده، رنو، عزت‌الله (۱۳۸۸)، «**تهدیدات اجتماعی و امنیت ملی**»، تهران: داعا.
- کاسلز، مانوئل (۱۳۸۰)، «**عصر اطلاعات، اقتصاد جامعه و فرهنگ**»، ج ۱، ترجمه احمد علی‌قلیان و افشین خاکباز، تهران: طرح نو.
- نای، جوزف، کیئن، رابرت (۱۳۹۰)، «**انقلاب اطلاعات، وابستگی متقابل و قدرت**»، ترجمه علیرضا طیب، تهران: پژوهشکده مطالعات راهبردی.
- نورمحمدی، مرتضی (۱۳۹۰)، «**گسترش فناوری‌های اطلاعات و ارتباطات و تحول امنیت**»، تهران: میزان.
- هاشمیان‌فرد، زاهد (۱۳۸۸)، «**امنیت در اسلام**»، دانشگاه عالی دفاع ملی، تهران.
- هایدگر، مارتین (۱۳۷۵)، «**پرسشی در باب تکنولوژی**»، ترجمه محمدرضا اسدی.

- Howard,v. perlmutter&tagi sagafi-nejad (۱۹۸۱),international technology transfer, new york,paragon press .
- Jeffrey R. cooper the coherent Battlefield removing the fog of war: a frame for understanding an MTR of the information age, Arlington, VA: SRS technologies, June ۱۹۹۳,p. ۲۳
- marx , Gary T (۲۰۰٤),some concept that may be useful in understanding the myriad forms and contexts ofsurveillance ,intelligence and national security quarterly , vole, summer
- Metz, s (۲۰۰۰), Armor conflict in the ۲۱st century: the information Revelation and postmodern warfare. Carlisle Barracks: strategic studies institute .
- Mitch man, coral (۱۹۹٤), thinking through technology: the path between Engineering and philosophy. Chicago: the university of Chicago Press .
- terverton,Gregory(۲۰۰۲),Reshaping national intelligence in an age of information ,Cambridge:Cambridge university press .