فضای سایبری: امنیت سخت یا امنیت نرم

فاطمه نوری*

عضو هیأت علمی گروه حقوق دانشگاه پیام نور، ایران

Email:NooriFatemeh90@yahoo.com

چکیده

باتوجه به ماهیت فضای سایبر بعنوان بستر اصلی اطلاعات کشور واینکه امکان صدمه زدن از این راه بسیار محتمل می باشد،لازم است که نگاه ویژه ای به مسأله ی امنیت فضای سایبر مخصوصا در سطح کاربردهای ملی شود زیرا زیرساخت های اصلی کشور در این فضا قرارگرفته است و بروز هرگونه مشکل امنیتی باعث تهدید جدی در امنیت ملی کشور خواهد گردید. مقاله حاضر با استفاده از روش تحلیلی به بررسی رویکردهای متفاوت امنیت (گاه نرم افزاری وگاه سخت افزاری)می پردازد . این بررسی نشان می دهدکه قدرت سخت ونرم با یکدیگر در ارتباط می باشند وهردو دارای جنبه هایی از قابلیت دستیابی به هدف بوسیله ی تأثیرگذاری در رفتار دیگران می باشند و تمایزبین آنها در ماهیت رفتار ودر غیرمحسوس بودن منابع می باشد به گونه ای که امنیت سخت یعنی قدرت می تواند برتوسل به زور ورفتاری دستوری متکی باشد امانمیت نرم یعنی تهدید شامل توانایی جذابیت وتوانایی کسب مطلوب از طریق جاذبه است نه از طریق اجبار .

کلید واژه ها:امنیت سخت ،امنیت نرم ، فضای بین المللی سایبری ،قلمرو حاکمیتی

International cyber space security hardware or software security

Fatemeh Noori

Member of scientific, Department of law, Payame Noor University, Iran

Abstract

Due to the nature of cyberspace as a mainstream information country is likely to offend in this way, it is important to look special . it is important to look special issue of cyber security, especially at a national application because of the country's infrastructure has been in this space and downtime security threat to n This paper examines the different approaches security using analytical methods (sometimes soft and sometimes hardware) address. The study show that the hardware can be connected to with aspects of accessibility to the target by influencing the behavior of others are ational security country And the nature and behavior of resources is strict security so that power can force order is based on the threat software includes the ability to obtain favorable interest through attraction rather than through coercion.

Keywords: hardware security, software security, international cyber space, territorial sovereignty

مقدمه

درکنار جهان واقعی ،جهان مجازی ظهورکرده که کنشگران دولتی و غیر دولتی فارغ از محدودیت های جهان واقعی در آن نقش آفرینی می کنند . برهمین اساس مارتین لیبیکی در کتاب خود باعنوان پیروزی در فضای سایبر : امنیت ملی ونبرد اطلاعاتی ،استدلال می کند که فناوری اطلاعات وارتباطات فضای جدیدی را در کنارجهان واقعی وعینی بوجودآورده که ازآن بعنوان فضای سایبر یاد می شود .مهمترین ویژگی فضای جدید کنترل ناپذیری تعاملات وتغییر ماهیت بسیاری از مفاهیم مانند قدرت وتهدید است.(Libicki,2007, P. 23)

منظور از فضای سایبر یا فضای مجازی ترکیبی از دهها هزار رایانه به هم پیوسته ،سرویس دهنده ها، شبکه های ارتباطی ،سوئیچ ها و کابلهای فیبر نوری است که امکان ایجاد ارتباطات را در یک سیستم جامع فراهم می آورد.کارآمد و سالم بودن فضای سایبر در کشورها از اهمیت ویژه ای برخوردار است.(افتخاری، 1382: 5)

جوامع امروزی به گونه ای فزاینده به این فضای مجازی وابسته شده اند.این در حالی است که حتی کشوری با تکنولوژی پیشرفته نمی تواند بطورکامل از حملات سایبری و تهدیدات وآسیب های آن در امان باشددوری جغرافیایی و مرز اهمیت خود را ازدست داده ،ظرف چند ثانیه می تواند مورد هدف قرار گیرد هر آنچه با عنوان تجارت و داد و ستد الکترونیکی،پول و بانکداری الکترونیکی،آموزش الکترونیکی،نشر الکترونیکی،انواع ارتباطات الکترونیکی، دادرسی الکترونیکی و حتی حکمرانی یا دولت الکترونیکی به کار می رود.همگی در فضای سایبر ریشه دارد و مجهز بودن هر کشور به آن جلوه ای از قدرت آن کشور می باشد.در حالی که هر کدام از آن ها نیز آسیب پذیر و در معرض تهدید بوده به گونه ای اصلاح و حمایت از آن ها اگر غیر ممکن نباشد؛بسیار دشوار خواهد بود.

در فضای سایبر کنشگران را به سه دسته می توان تقسیم کرد :حکومتها،نهادهای دارای شبکه های سازمان یافته و افراد و شبکه هایی با ساختارضعیف که در این میان خود فضای سایبر یک منبع قدرت محسوب می شود .فضایی که در ابتدا تنها انتظاری که از آن می رفت محاسبه ی دقیق اطلاعات و ارائه نتایج در کمترین زمان ممکن بود اما به تدریج احراز شد که قابلیت فضای سایبری به مراتب بیش تر و متنوع تر است.همین انعطاف پذیریبی نظیر باعث شد برای امور خرد و کلان مختلف برنامه های رایانه ای مناسبی طراحی و تولید شود و فضایی با کارایی و اثر بخشی غیر قابل مقایسه ای نسبت به فضای حقیقی به اجرا در آید.

به همین دلیل به کارگیری فضای سایبری بر فضای فیزیکی و حقیقی غلبه یافت .شبکه های کوچک و بزرگ رایانه ای شکل گرفت و تقریباً تمامی امور ملی و داخلی کشور ها در یک بستر مشترک و واحد در عین حال جهانی اداره گردید. ایجاد این قدرت برای کشورها بزرگترین دستاورد فناوری اطلاعاتی و ارتباطی هزاره ی نوین است که همگام با توسعه ی جهانی بطور مستمر در حال دگرگونی و نو شدن است.از طرف دیگر تهدیدهای

سایبری تقریباً تمامی کشورها را به یک اندازه هدف قرار می دهد و شاید کشورهای پیش روی این عرصه که همان کشورهای توسعه یافته هستند بیشتر از این تهدیدها آسیب می بینند.به همین جهت در کنار قدرت سایبری،مقابله با تهدیدهای سایبری بعنوان یک آسیب ،به دغدغه ی کشورهای توسعه یافته تبدیل شده است زیرا این فضا بطور لحظه شمار در حال نو شدن است .و کشوری می تواند به حیات سایبری اش ادامه دهد که جلوه ی فعال و کنشی قابل قبول در سطح بین المللی بیاید.(Shinder,2002,P.246)از آنجا که فعالیت های سایبری گوناگون و متنوع می شود باید ابزارهای موجود توانایی خنثی سازی آثار سوء این فعالیت ها را داشته باشد .برای مثال ابزارهای فیلترینگ بر اساس فهرست های سفید یا سیاهی عمل می کنند که هر کشور بر اساس قوانین داخلی اش تدارک دیده است .بسیار محتمل که به هنگام راه اندازی و به کارگیری این ابزارها در کشور دیگر،بخشی از اطلاعات غیر قانونی هم چنان در دسترس باشد یا بخشی از اطلاعات قانونی غیر قابل دسترس شوند .زیرا قوانین داخلی در کشور بر اساس ارزش ها و منافع ملی آن تدوین می شوند و لزوماً مشابه سایر کشورها نیستند. (جلالی فراهانی، 1386: 6)

در دنیای فیزیکی و حقیقی ،کشورهای جهان با هدف احترام متقابل به حاکمیت ملی یکدیگر،از انجام اقدامات اجرای قانون در قلمرو یکدیگر پرهیز و در صورت لزوم و در مواقع استثنایی،طبق ضوابط خاصی عمل می کنند.(کریانگ ساک کیتی ،1383: 16) اما در فضای سایبر،این وضعیت خاص و استثنایی است.زیرا هر گونه ابتکار عمل کشورها،با حاکمیت ملی چندین کشور دیگر در تعارض قرار می گیرد.از طرفی نیز پایبندی به موازین حقوقی ایجاب می کند.مسیر جدیدی برای این حوزه ی نو پدید وتعریف شود.تا نظم و امنیت ملی کشورها نیز حفظ گردد.

در این نوشتار گستره ی فرامرزی فضای سایبر بعنوان امنیت سخت (قدرت) یا امنیت نرم یعنی تهدید بررسی می شود، به همین منظور مباحث به دو بخش تقسیم شده است.بخش نخست به استفاده ی کشورها از فضای سایبری و انجام اعمال سایبری که نشانه ی امنیت سخت و قدرت آنان است گزینش شده اند و بخش دوم نیز تهدیدات ناشی از استفاده از فضای سایبر وانجام اعمال سایبری در قلمرو حاکمیت ملی کشورها مورد بررسی قرارمی گیرد و در پایان نیز با توجه به مباحث مطروحه نتیجه گیری بعمل می آید.

1: امنیت سخت در فضای سایبر

در فضای سایبر، ازمقوله ی امنیت سخت به نام قدرت یاد می شود که به این صورت تعریف می شود:«استفاده ی طراحی شده از تبلیغات و فعالیت ها جهت تأثیرگذاری عقاید،نگرش ها،احساسات و رفتار گروههای خارجی به شکلی که از اهداف ملی حمایت و در افکار عمومی نیز کسب اعتبار نماید(نای ، 1382: 65) قدرت متقاعد کردن مردم و شکل دهی افکار آنان بصورت فرماندهی وتوانایی تغیی آنچه دیگران انجام می دهند .

در عصر سایبر،جهان جدید به شبکه ی نیرومندی تبدیل شده است که بافت اصلی و تاروپود آن را اطلاعات و نظام ارتباطات الکترونیک تشکیل می دهد .در درون این شبکه به جز گروهی از نخبگان دیگران کنترل خود را بر زندگی خویش و محیط پیرامون از دست داده اند یا به سرعت در حال از دست دادن هستند.

از چشم انداز ارتباطات بین المللی می توان امنیت سخت یا قدرت را در مرحله ی روابط بین المللی به سه دسته ی کلی تقسیم کرد:قدرت نظامی،قدرت اقتصادی،قدرت نرم که هریک از این سه نوع قدرت برای مقاصد خاص،با نمودارهای رفتاری متفاوت و در سیاست های مختلفی بوسیله ی حکومت ها اعمال می شوند.قدرت نظامی به قصد اجبار و بازدارندگی طرف مقابل و از طریق دیپلماسی قهر آمیز اعمال می گردد.قدرت اقتصادی به قصد ایجاد نوعی برانگیختن کشورهای خاص و از طریق تشویق یا تحریم اقتصادی یا تضییع و کمکهای مالی اعمال می شود اما قدرت نرم با نیت ایجاد جذابیت برای خود و تنظیم اولویت های طرف مقابل بوسیله ی ابزارهایی مانند فرهنگ ،انتقال ارزشها و نهادهای اجتماعی و از طریق دیپلماسی عمومی اعمال می شود. (احمدزاده کرمانی ، 1387: 44)

قدرت نرم بر خلاف قدرت نظامی که دارای ساختارهایی با منطق سلسله مراتبی و از سمت بالا به پایین است ،در ساختار دایره ای و فاقد اضلاع تعریف می شود که در آن بر خلاف مدل سلسله مراتبی-که امکان دیالکتیک تمام اجزا در آن واحد میسر نیست-منطق دیالکتیک در آن باز تولید می گردد.(افتخاری،1387: 18)

هریک از کنشگران دولتی و غیر دولتی در سطح بین المللی به یکی از روشهای فوق امنیت سخت را به اجرا می گذارند به هرحال استفاده از فضای سایبری و انجام اعمال سایبری،نشاندهنده ی تسلط و قدرت کشورها در سطح ملی و بین المللی است این حوزه ی بدون مرز ، استلزامات بین المللی و نحوه ی همکاری و معاضدت یک کشور با سایر کشورها را نشان می دهد و فضای سایبر یک بستر مشترک جهانی را بوجود می آورد که هر کشور در هر گوشه ی جهان می تواند فعالیت مورد نظر خودرا به آن منتقل و از مزایای بی شمار آن بهره برداری کند طبیعتاً در چنین وضعیتی تأثیرپذیری و تأثیر گذاری امور سایبری بر یکدیگر ،به اندازه ی همان گستره ی جهانی خواهد بود.از طرف دیگر یکی از اصول ابتدایی که مورد توافق همه ی کشورهای جهان قرار گرفته است احترام متقابل به حاکمیت ملی و پرهیز از مداخله در قلمرو حاکمیتی یکدیگر است.در حالیکه پیدایش فضای بدون مرز سایبر مسائل اساسی را ایجاد نموده است به گونه ای که کشورها نام دامنه ی وب سایت مورد نظر را به نام دامنه ی ملی (مانند ir.) می شناسندکه خود نشاندهنده ی حاکمیت ملی آن کشور می باشد.یا اینکه در کنار نام های دامنه ملی ،نام های دامنه ی عمومی (مانند com.)قرارمی دهندکه عموماً وب سایت هایی هستند که مخاطب محتوای آن ها مستقیماً اتباع یک کشور می شود و به سایر کشورها مربوط نمی شود.ودر عمل نیز کشور ها به خود اجازه نمی دهند که ادعای صلاحیت در این خصوص بنمایند حتی بسیاری از کشورها در قلمرو

حاکمیتی خود در فضای سایبر اقدام به ارائه اعتبارهای پست الکترونیکی به اقشار خاص مانند دانشجویان یا کارکنان نموده اند که همه ی این ها ماهیت فرامرزی فضای سایبر را به عنوان موضع قدرت یک کشور در قبال سایر کشورها نمایان می سازد.

2 : امنیت نرم در فضای سایبر

امنیت نرم یا تهدید در عرصه ی سایبری تحولاتی است که موجب دگرگونی در هویت فرهنگی و الگوهای رفتاری مورد قبول یک نظام سیاسی می شود.تهدید در واقع نوعی زمینه ی مسلط در ابعاد سه گانه ی حکومت ،اقتصاد و فرهنگ است که از طریق استحاله الگوهای رفتاری در این حوزه ها و جایگزینی الگوهای نظام سلطه محقق می شود.(احمدزاده کرمانی ، 1388: 143)

معمولا امنیت سخت متکی بر روشهای فیزیکی،عینی،سخت افزارانه و همراه با اعمال و رفتارهای خشونت آمیز و با قصد بر اندازی آشکار و با استفاده از شیوه ی اجبار و اشغال سرزمینی صورت می گیرد.برخلاف تهدید که بدون منازعه و لشکر کشی فیزیکی انجام می گیرد و محصول پردازشی ذهنی نخبگان این حوزه وسایل اجتماعی،فرهنگی و سیاسی است.(نایینی ، 1387: 57)

تغییرات حاصل از تهدید ما هوی ،آرام ،ذهنی،تدریجی و نرم افزارانه است. تهدید همراه با آرامش و خالی از روش های فیزیکی و با استفاده از شیوه ی القاء مجاب سازی و اقناع و در بستر های قانونی بدون ایجاد حساسیت و برانگیختن اعمال می شود.

در مجموع می توان نقاط افتراق امنیت سخت و نرم را اینگونه برشمرد:

1-حوزه ی امنیت نرم،حوزه ی اجتماعی،فرهنگی و سیاسی است.

2-امنیت نرم محصول پردازشی ذهنی نخبگان و اندازه گیری آن مشکل است.

3-روش اعمال تهدید ،بهره گیری از مدل های روانشناختی در تغییر رفتار،مجاب سازی به القاء و قانع سازی است.

4-امنیت نرم به دلیل ماهیت غیر دینی و محسوس آن ،اغلب فاقد عکس العمل است یعنی مسالمت آمیز بوده و جنبه ی غیر خشونتی دارد.و بنابر این حوزه های سطحی ،حمایتی را در جامعه و حکومت بر نمی انگیزد.

5-ارزیابی پیامدهای امنیت نرم و تشخیص میزان شکست و پیروزی آن ،بسیار سخت است.(مرادی، 1388: 38 و 99)

امنیت نرم امروزه با بهره گیری از حوزه هایی چون:دیپلماسی عمومی،دیپلماسی رسانه ای و مجازی (تصویر سازی) تجربه ی کاملاً متفاوتی از رویارویی کشورها را به منصه ی ظهور رسانده است.به این معنا که بازیگران

سعی می کنند با استفاده از فناوری های نوین ،از رقیبان خود «تصویر مجازی» تولید کنند که امکان جایگزین شده با واقعیت را داشته باشد.(عبدالله خانی ، 1386: 139)

تهدید اطلاعاتی ،تهدید اجتماعی ،تهدید سیاسی ،تهدید فرهنگی ،تهدید روانی،تهدید رایانه ای وتروریستی رامی توان از جمله مصادیق امنیت نرم به شمار آورد.

ابعاد اطلاعاتی امنیت نرم

استفاده از فضای سایبر در ابعاد مختلف تهدیدی جدی محسوب می شود دربعد اطلاعاتی ،گزینه های فراوان برای بررسی وجود دارد.مانند دسترسی آسان به سایت های جاسوسی آمریکا ،اسرائیل و کشورهای دیگر امکان ارسال و دریافت ایمیل به هر نقطه از دنیا و غیر قابل کنترل بودن داده های مبادله شده ،باعث شده که خود سیستم اطلاعاتی و امنیتی مورد دستبرد اطلاعاتی قرار گیرد .

ابعاد اجتماعی امنیت نرم

ارتباطات نامتقارن و غیر اخلاقی جوانان،گسترش شبکه های مجازی تجارت الکترونیک (آنچه به نام گلدکوئیست و پنتاگون شناخته شده است)گسست میان نسلی،بی هویت سازی تهدید بنیان های خانوادگی ،شکل گیری خرده فرهنگ مختلف ،تحریک پذیری و قومیت ها .

ابعاد سیاسی امنیتنرم

ایجاد گروههای سیاسی مجازی انتقال مستقیم اندیشه ها و دیدگاههای جریان های معاند به داخل،ایجاد گروههای فشار و ذی نفوذ مجازی،دموکراسی دیجیتالی ،مکانیسم های شایعه سازی و بی اعتبار سازی مرزها،افزایش همگرایی گروههای داخلی و خارجی هم فکر علیه نظام.

ابعاد فرهنگی امنیت نرم

فضای سایبر در بعد فرهنگی به صورتهای زیر تهدید به شمار می آید:

1-کاهش نفوذ رسانه های ملی و داخلی

2-ایجاد محرک های قوی برای تبادلات فرهنگی غیر قابل کنترل

3-بستر سازی بیشتر برای تهاجم فرهنگی

4-انتقال هنجارها خرم های ارزشی و اخلاقی غربی

5-جایگزینی رسانه ای (مجیدی ، 1381: 125- 127)

ابعاد رایانه ای امنیت نرم

*تهدید رایانه ای باعنوان سایبر تروریسم نخستین بار از طرف کالین باری (Collin barrg)*دردهه ی 1980 مطرح شد.ولی گفته می شود جامعترین تعریف از سوی «دوروتی دلینگ» استاد علوم رایانه ای دانشگاه جرج تاون ارائه شده است :«سایبر تروریسم بیشتر به معنای تهدید رایانه ها ،شبکه های رایانه ای و اطلاعات ذخیره شده در آن هاست .هنگامی که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی و اجتماعی خاص اعمال می شود.»اساسی ترین روش های سایبر تروریسم عبارتست از :هک کردن ،ویروس های رایانه ای،جاسوسی الکترونیک ،دزدی هویت و تخریب یا دستکاری اطلاعات. (عزیزی ،1388: 122)

سایبر تروریسم ناشناخته تر از روش های تروریسم کلاسیک است.مانند بسیاری از کاربران اینترت تروریست ها از اسامی مستعار استفاده می کنند و بعنوان کاربر ناشناس به یک سایت و صل می شوند.سایبر تروریسم می تواند شبکه های دولتی ،شخصی،خدمات عمومی و هوایی را مورد حمله قرار دهد.از راه دور کنترل شده و توانایی زیادی در جهت جذب تعداد زیادی از مردم را به خود دارد.

نتیجه گیری:

حوزه ی سایبر یک محیط جدید ،مصنوعی وغیر قابل پیش بینی است ،دنیایی بی نظیر که با وجود مزایای شگفت انگیز برای جامعه ی بشری ، تهدیدی جهانی محسوب می شود آن هم به دلیل بین المللی یا فرامرزی بودن آن .زیرا مجرمان سایبری بدون محدودیت و با بهره وری باورنکردنی،اهداف مجرمانه شان را پیش می برندواین،در حالی است که کشورها خود،مسؤول حفظ نظم و امنیت جامعه ی خود بوده و در برابر زیان های سهمگین سوء استفاده های سایبری پاسخگو هستند و بایستی مقابله با انواع تهدیدات سایبری را سر لوحه ی برنامه های اصلی خود قرار دهند و در امر جرم انگاری سایبری یا اصلاح قوانین فعلی خود نقش اساسی داشته و بعنوان دغدغه ی مقامات حاکمیتی به آن بنگرند تا از بروز چنین تهدیداتی جلوگیری کنند.

لذا مهمترین مرحله در جلوگیری از تهدیدات و حملات سایبری آموزش عمومی ،امنیتی وپلیسی است.زیرا نه تنها مردم عادی بلکه احتمالاً بسیاری از مقامات هیچگونه اطلاعات در مورد حملات فضای سایبر و چگونگی آن ندارند لذا باید در مورد ایمن کردن فضای سایبر آنها را متقاعد کرد و با آگاهی دادن به مردم آن ها را وادار کرد تا تمهیدات لازم را برای مقابله با تهدیدات سایبری اعمال کنند.

علاوه بر سازو کار فوق در مرحله ی بعد باید سازوکار حقوقی و قضایی مناسبی را برای مقابله با تهدیدات سایبری ایجاد کرد.مانند از بین بردن خلأهای قانونی نیروی امنیتی و قضایی و تقویت دفاعی سازمان های مقابله کننده با حملات و تهدیدات سایبری.

International cyber space security hardware or software security

Abstract

Due to the nature of cyberspace as a mainstream information country is likely to offend in this way, it is important to look special . it is important to look special issue of cyber security, especially at a national application because of the country's infrastructure has been in this space and downtime security threat to n This paper examines the different approaches security using analytical methods (sometimes soft and sometimes hardware) address. The study show that the hardware can be connected to Vhrdv with aspects of accessibility to the target by influencing the behavior of others are ational security country And Tmayzbyn the nature and behavior of resources is Ghyrmhsvs strict security so that power can force Brtvsl BEHAVIORAL order is based on the threat Amaamnyt software includes the ability to obtain favorable interest through attraction rather than through coercion. Keywords: hardware security, software security, international cyber space, territorial sovereignty.

Keywords: hardware security, software security, international cyber space, territorial sovereignty

فهرست منابع

فارسی

1-احمدزاده کرمانی،روح الله،محمد صادق اسماعیلی.(1387) . **فرهنگی شدن سیاست خارجی:رویکردی نرم اقتدارانه**،تهران.پژوهشکده ی مطالعات و تحقیقات بسیج دانشگاه امام صادق (ع).

2- احمد زاده کرمانی.(1388).**درآمدی بر ماهیت شناسی جنگ نرم و پس از انقلاب ایران**.فصلنامه ی مطالعاتی بسیج.شماره ی 43.

3- افتخاری،اصغر .(1382).**استراتژی ملی برای تأمین امنیت در فضای مجازی**، تهران ،پژوهشکده ی مطالعاتراهبردی.8

4-افتخاری،اصغر.(1387).**قدرت نرم**.تهران.پژوهشکده ی مطالعات و تحقیقات بسیج دانشگاه امام صادق (ع).

5- جلالی فراهانی،امیر حسین.(1386).**تأملی بر فیلترینگ :1.اقدام پیشگیرانه از جرایم رایانه ای**.مرکز پژوهش های مجلس شورای اسلامی، شماره ی 8371.

6-عزیزی،مرتضی. (1388).**سایبر تروریسم یا تروریسم اینترنتی**، تهران ،معاونت سیاسی نهاد نمایندگی مقام معظم رهبری در دانشگاه.

7- عبدالله خانی ، علی . (1386). تهدیدات امنیت ملی، تهران ، مؤسسه مطالعات و تحقیقات بین المللی ابرار معاصر ایران .

8-کریانگ ساک کیتی ، شیایزری.(1383).**حقوق بین المللی کیفری**،ترجمه ی بهنام یوسفیان و محمد اسماعیلی.چاپ نخست .انتشارات سمت.تهران.

9-مجیدی،عبدالله .(1381).**نقش رسانه ای اینترنت در نا امنی های اجتماعی**،تهران،معاونت سیاسی نهاد نمایندگی مقام معظم رهبری.

10-مرادی،حجت الله.(1388).**قدرت جنگ نرم از نظریه یا عمل** ،تهران:انتشارات ساقی.

11 -نای،جوزف.(1382).**قدرت نرم**.ترجمه ی محمد حسینی مقدم .فصلنامه ی راهبرد.ش 29.

12-نائینی،علی محمد.(1387). **قدرت و تهدید نرم در مطالعات امینی**. جلد اول ،مجموعه ی مقالات قدرت نرم .تهران.پژوهشکده ی مطالعات بسیج.

لاتین

1- Libicki,MartinC.conquest in Cyberspace;national security and information warfare,London:Cambridge university press,2007

3-Shinder,DebraLittlejohn,scene of the cyber crim,computer forensics Handbook,syngress publication,2002