حرب المعلومات

ماهيتها – انواعها – مستوياتها

م . م سراب ثامر أحمد

.

الملخص

يتناول هذا البحث بالدراسة موضوع (حرب المعلومات) التي تعرّف بانها (الاعمال التي تنفذ للتأثير على معلومات العدو ونظم معلوماته ووظائفها ، او انكارها او استغلالها او تدميرها وفي نفس الوقت حماية المعلومات ونظم المعلومات الخاصة بالمهاجم).

وتشتمل هذه الحرب على تقنيات تقليدية كالخداع والتمويه والهجمات المادية على واقع المراقبة وخطوط اتصالات العدو ، الا إن تطور تكنولوجيا المعلومات كأجهزة الحاسب الالي ، الاتصالات والشبكات الالكترونية جعل من الممكن للخصوم استهداف بعضهم بطرقٍ وتقنيات جديدة كاستخدام تقنية انكار الخدمة او الفايروسات او القنابل المنطقية ... الخ لغرض استغلال او تدمير او تعطيل معلومات العدو ونظم معلوماته دون اي حاجة لدخول اقليم دولة ودون التمييز بين الاهداف المدنية والعسكرية.

Abstract

The subject of this research is the " Information Warfare " , which can be defined as " any action to deny , exploit , corrupt or destroy the enemy's in formation and its functions , protecting ourselves against those actions ".

This warfare includes both old techniques such as ruses , Camouflage and physical attacks on observation Posts and Lines of Communication.

The development of information technology , specifically Computers , telecommunications , and networks makes it possible for adverse arise to attack each other in new ways and with new techniques , such as the denial of services , viruses , logic bombs … etc to destroy or exploited the enemy's information and information systems without ever physically entering the enemy's country and without distinguishing between military and Civilian targets.

مقدمة

ان الحروب المعلوماتية قديمة قدم النزاع البشري ، فالدوافع الكامنة وراءها بقيت عل حالها عموماً ، فالسعي لتقويض ثقة الخصم ، وتعطيل خطوط اتصالاته وإرباكها وخلق الأوهام في نفسه بشأن النزاع ومسرحه ، لكنها دوافع قائمة في عالم اليوم إلا ان ما استُجد في القرن الحادي والعشرين هو شيوع البنى التحتية المعلوماتية الالكترونية الرقمية مما أدى إلى شراسة الهجمات المعلوماتية التي يمكن أن تمزق النسيج الاجتماعي للبلد المستهدف إلى جانب القدرة على إلحاق أضرارٍ مادية واسعة بسبب الطاقات والقدرات التدميرية للهجمات المعلوماتية المتواصلة والمتاحة للجميع من أفراد أو مؤسسات أو دول. وعلى مدى العقدين الماضيين قامت البلدان الصناعية بنشر شبكات واسعة من الأصول الاقتصادية والمادية والاجتماعية الهامة المربوطة عبر تكنولوجيا المعلومات والاتصالات للنهوض بمستوياتها المعيشية والاقتصادية وقوتها على المستوى الدولي إلى جانب ان ذلك احدث ثورة في الشؤون العسكرية فيما يتعلق بتغيّر سبل تخطيط الحروب وتنظيمها وإدارتها وتطور القدرات على تنفيذ مهام جمع المعلومات وتحليلها والمراقبة والاستطلاع وقيادة القوات واستخدام الأسلحة الذكية ، وفي مقابل ذلك نشأت طرق جديدة للأنشطة غير المشروعة باستخدام أسلحة تقنية ذات طبيعة خاصة تلاءم التطور التكنولوجي لاستغلال نقاط الضعف التي تنطوي عليها أنظمة التشغيل والبرمجيات مما يفتح الباب لإمكانية القيام بأعمال تهدد الخدمات الأساسية للسكان المدنيين وتسهل التجسس الاقتصادي وتؤثر على مصداقية تكنولوجيا المعلومات والاتصالات وقدرة المجتمعات على العمل ، مما يثير تحدّيات جديدة للأمن القومي والاقتصادي ويؤدي وبالتالي إلى تدمير البنية التحتية بأكملها وتعطيل الاتصالات إضافة إلى أن ضعف النظم التكنولوجية قد يمثل تهديداً حقيقياً لأمن الدول.

ولدراسة حرب المعلومات ارتأينا تقسيم خطة البحث على مبحثين نتناول في المبحث الأول مفهوم حرب المعلومات بينما خصصنا المبحث الثاني للبحث في أنواع حرب المعلومات ثم استتبعنا ذلك بخاتمة.

المبحثالأول

مفهوم حرب المعلومات Information Warfare

ظهر مصطلح حرب المعلومات لأول مرة عام ١٩٧٥ ، حيث أدركت الدول المتقدمة تقنياً أهمية ذلك وسعت الى تطبيقه في المجالات السياسية والعسكرية والاقتصادية والثقافية. وفي اواخر التسعينات من القرن الماضي ظهر مصطلح اوسع من حرب المعلومات وهو العمليات المعلوماتية (Information Operation) ولبحث ذلك قسمنا هذا المبحث الى مطلبين ، المطلبالأول يتناول التعريف بحرب المعلومات والعمليات المعلوماتية والمطلب الثاني يتناول ادوات تعقب وجمع وافساد المعلومات ومستويات حرب المعلومات.

المطلب الاول

تعريف حرب المعلومات والعمليات المعلوماتية

Definition of Information Warfare

and Information operations

أولاً : العمليات هي اية عملية عسكرية او غير عسكرية هدفها السيطرة على تفكير الخصم لدفعه الى اتخاذ قرار وتنفيذه بطريقة تخدم مصلحة الطرف الاخر ، ومنعه في ذات الوقت من ممارسة تلك العمليات ضده اما الخصم فقد يكون دولة معادية ، او دولة صديقة او تنظيماً منافساً او حتى شخصاً متطفلاً.

وعليه فان العمليات المعلوماتية (I O) هي (الاعمال التي تنفذ للتاثير على معلومات العدو ونظم معلوماته ، وفي نفس الوقت حماية المعلومات ونظم المعلومات الخاصة بالمهاجم).

وتشتمل هذه العمليات على اية اجراءات تتخذ بغير رضا متبادل بين الطرفين (المهاجم والمستهدف)، والغاية من وراء ذلك هو اكتشاف البيانات المُخزّنة في احد اجهزة الحاسب الآلي او تغييرها او تدميرها او تشويهها او تحويلها او البيانات التي تستخدم او تنقل عن طريق احد الاجهزة ويمكن ان يحدث ذلك في اوقات النزاع والازمات او في اوقات السلم على حد سواء على

المستويات الاستراتيجية حيث يمكن ان تستخدم العمليات المعلوماتية لتحقيق اهداف وطنية بالتاثير على جميع العناصر (السياسية او العسكرية) او الاقتصادية او المعلوماتية للقوة الوطنيةللعدو المحتمل ، وفي نفس الوقت حماية العناصر المماثلة الصديقة.

ويمكن ان تجري العمليات المعلوماتية على المستوى العملياتي حيث يكون التركيز على خطوط اتصال العدو والاعمال اللوجستية والادارة والسيطرة والقدرات والانشطة ذات الصلة وفي نفس الوقت حماية العناصر المماثلة الصديقة.

والمستوى التكتيكي للعمليات المعلوماتية هدفه اصابة المعلومات ونظم المعلومات الخاصة بالعدو والتي تتعلق بالادارة والسيطرة والتخابر وغيرها من العمليات التي تعتمد على المعلومات بشكل مباشر والتي تتعلق بسير العمليات العسكرية[١].

ثانياً : (I W) اما حرب المعلومات فهو مفهوم اضيق من العمليات المعلوماتية لانها تُعرف بانها (عمليات معلوماتية تجري اثناء الازمات او النزاع لتحقيق او تعزيز اهداف معينة ازاء عدو او اعداء محددين).

فالاختلاف يتمثل بالسياق الذي تجري فيه حرب المعلومات والذي ينحصر في حالة النزاع على خلاف المصطلح الاول الذي قد يجري في حالات السلم أيضاً. فعمليات التجسس الروتينية التي تحدث في اوقات السلم على سبيل المثال تُعد عمليات معلوماتية ولكنها لا تمثل حرب معلومات الا اذا جرت في اثناء ازمة او خلال الاعمال العدائية[٢].

وحرب المعلومات تمثل اي هجوم ضد توظيف او تفعيل المعلومات لدى الخصم لحرمانه منها وتدميرها ووظائفها ومنها مثلاً القيام بتفجير شبكة التليفونات عن طريق الضربات الجوية وبالمقابل القيام بحماية تلك الشبكة يدخلان في نطاق هذه الحرب فالاول يمثل هجوماً لحرمان العدو من معلوماته والاخر يمثل اجراء دفاعياً لحماية النفس من ذات الفعل.

ويشير مصطلح حرب المعلومات الى استخدام المعلومات او الهجوم عليها كشكل من اشكال الحرب ، فهذه ترى في المعلومات نفسها حقلاً او كيانً منفصلاً ومستقلاً اما كسلاح في حد ذاته ، واما كهدف في ذاته ، وهي بذلك تختلف عن مصطلح (الحرب في عصر المعلومات) الذي يستخدم بدوره تكنولوجيا المعلومات كأداةٍ تمدُ اطراف النزاع برسائل غير مسبوقة من حيث القوة والسرعة والدقة في تنفيذ العمليات العسكرية التي قد تستهدف اهدافاً لا علاقة لها بالمعلومات او نظمها[٣].

هذا وقد ذهبت الاستراتيجية القومية العسكرية للولايات المتحدة الى تعريف حرب المعلومات بأنها (الاعمال التي تتخذ لتحقيق تفوق المعلومات عن طريق التأثير على المعلومات المعادية

والعليات المبنية على هذه المعلومات ونظم المعلومات ، وفي نفس الوقت حماية المعلومات والعمليات المبنية عليها ونظم المعلومات الخاصة بالمهاجم). ومن الواضح من التعريف أن هذه الاستراتيجية نجد أن التفوق المعلوماتي (Information Superiority) هو عنصر اساس لهذه الاستراتيجية فهو تمثل (القدرة على جمع ومعالجة ونشر تدفق متواصل من المعلومات المحددة التي يمكن الاعتماد عليها وفي نفس الوقت استغلال وحرمان العدو من القدرة على عمل الشيء نفسه)[٤].

ومن جانب اخر فان دليل القوات الجوية الامريكية ذكر مفاهيم متعددة في اشارة لاستخدام حرب المعلومات ومنها (الافساد والخداع) الذي يمثل تغيير المعلومات او التلاعب بالبيانات لجعلها غير دقيقة وبلا معنى (والتاخير والحرمان) الذي يشير الى الابطاء في تدفق المعلومات او وقفها لفترة من الزمن ، اضافة الى (احداث الاضطراب والاضعاف والتدمير) الذي يرمي الى خفض القدرة على تقديم ومعالجة المعلومات او تدميرها قبل أن يمكن نقلها والقضاء الدائم على القدرة على توفير ومعالجة المعلومات[٥].

المطلب الثاني

ادوات تعقب وجمع وافساد المعلومات ومستويات حرب المعلومات

أولاً : ادوات تعقب وجمع وافساد المعلومات

من المعلوم ان تنفيذ اية عملية عسكرية بسيطة كانت او معقدة ونجاح تنفيذها ، يعتمد بالدرجة الاولى على مدى دقة وحداثة المعلومات المتوافرة لدى الجهة المنفذة ، حيث تعد هذه احدى اهم عناصر التفوق واحراز الميزة العسكرية. وهذه تتطلب ادوات لجمع المعلومات التي تنقسم بدورها الى ادوات لتعقب وجمع المعلومات من خارج نطاق البنية المعلوماتية الاساسية للعدو واخرى تمثلها ادوات وتستخدم للجمع من داخل تلك البنية الاساسية.

فالقسم الاول يتمثل باستخدام الوسائل التقليدية كالجواسيس وعناصر المخابرات ، وان كان دورهم قد تطور الى زرع المستشعرات والاجهزة المتقدمة لامداد الاسلحة الذكية بالمعلومات اللازمة للتدمير ، والمثال الاخر لهذا القسم تمثله وسائل الاستطلاع الحديثة ، كالاقمار الصناعية ، حين تظهر الاستعمالات العسكرية لهذه الاقمار في الاستطلاع والتصوير ومراقبة اهداف معينة على الارض والقيام باجراء البحوث الي تحتاجها السلطات العسكرية وفي ربط

اشارات التلفزيون والرادار وفي اطلاق وارشاد الصواريخ وفي التحذير المبكر بالهجوم على الدولة ، الى جانب استخدام تلك الاقمار في التشويش على ما يصدر من الاقمار الاخرى او عن مراكز سطح الارض اشارات او موجات بالراديو او التلفزيون او الرادار ، ومن الصعوبة التمييز بين الاقمار الصناعية التي تستخدم لاغراض الرصد الجوي وبين تلك التي تُطلق للتجسس وجمع المعلومات او تلك التي تطلق للقيام بالمهمتين معاً[٦].

ومن الوسائل الحديثة الاخرى الرادارات العملاقة والطائرات بدون طيار التي يمكن استخدامها في المجالات العسكرية لتوفير معلومات دقيقة نسبياً عن الاهداف المراد استهدافها ، فهذه الطائرات التي يمكن ان يتم توجيهها لاسلكياً او أن تكون ذاتية التحكم ، يمكن ان توفر مسحاً متواصلاً لساحات الحرب من خلال النقل المباشر لما يجري فيها الى مراكز القيادة والسيطرة والى طائرات الدعم الجوي الغربية ، وهذه تؤدي الى الاستفادة من المعلومات المتحصلة من اجهزة استشعار الطائرات بدون طيار[٧].

القسم الاخر لادوات تعقب وجمع المعلومات من داخل البنية الاساسية للعدو والمتمثلة بشبكات الاتصالات والمعلومات وقواعد البيانات ونظم المعلومات والتحكم والسيطرة والتي تحتاج بدورها الى وسائل مختلفة تناسب طبيعتها ومن تلك الوسائل استغلال البوابات الخلفية او ما يعرف بـ (Trap Doors) التي تمثل ثغرات في برنامج الكتروني معين يتيح للمخترق الوصول من خلال النظام ، او قد تتمثل بالفيروسات والقنابل المنطقية وكذلك عمليات التقلص على شبكا المعلومات باختراق دفاعات الشبكات واستراق الامواج باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف انواعها كالتقاط موجات شاشات الحاسب الالي الضوئية او التقاط الموجات الصوتية من اجهزة الاتصال[٨].

الى جانب القسمين السابقين ، فان هناك ادوات لافساد وتعطيل المعلومات فهذه تشتمل على الدعاية المباشرة وضخ المعلومات المضللة او استخدام الاسلحة العادية ضد اهداف معينة لاجل تعطيل وافساد ما يمتلكه العدو من معلومات[٩].

ثانياً : مستويات حرب المعلومات واسلحتها

تنقسم حرب المعلومات الى ثلاثة مستويات هي :

أ . حرب المعلومات الشخصية.

هذا المستوى يصف الهجوم ضد الخصوصية الالكترونية الفردية مما يشكل اعتداء على الحقوق الشخصية للفرد وحرمة الحياة الخاصة ومنها سرقة البيانات المالية ونشرها عبر الشبكة الالكترونية للمعلومات (الانترنت) او قيام احد الاشخاص بتكوين ملف ن طريق الحاسب الالي يحتوي معلومات اسمية تخص شخصاً اخر بغير علمه او اذنه ، القيام على البريد الالكتروني للفرد لمراقبة شؤونه الالكترونية ، او العبث بالسجلات الرقمية وتغيير مدخلاتها المخزونة في قواعد البيانات[١٠].

بـ حرب المعلومات بين الشركات والمؤسسات

وهذا المستوى يدور ضمن اطار المنافسة بين الشركات والمؤسسات قوامها استباقةكل شيء لتعطيل المنافس وتهديد اسواقه. فقد تقدم شركة معينة باختراق النظام المعلوماتي لمنافستها وسرقة نتائج وتفاصيل ابحاثه وتدمير البيانات الخاصة ب هاو استبدالها ببيانات اخرى غير صحيحة.

جـ . حرب المعلومات العالمية

وهذا المستوى يمثل الحروب التي تنشب بين بعض الدول او الذي قد تشنه القوى الاقتصادية العالمية على بلدان بعينها بغية سرقة اسرار الخصوم او الاعداء وتوجيه تلك المعلومات توجيهاً مضاداً لمصالحهم.

هذا ومهما كان نوع حرب المعلومات . ضد فرد او مؤسسة اودولة . فلابد من وجود اسلحة تستخدم لتنفيذ هذه الحروب.

وقديما كانت الاساليب التقليدية تتمثل باستخدام الاطراف من الدول مثلاً وسائل التمويه لتضليل مراقبة الاعداء او القيام بقطع خطوط التلغراف الواصلة بين طرفي الحرب اضافة الى الاستهداف بالهجمات المادية التقليدية لنظم المراقبة التابعة للعدو كرادارات مثلاً.

الا ان التطور في مجال تكنولوجيا المعلومات وعلى وجه الخصوص الحواسيب . وسائل الاتصال والشبكات الالكترونية ، جعل م الممكن القيام باستهداف الخصم . فرداً او دولة او مؤسسة . باساليب جديدة تلائم طبيعة ذلك التطور[١١].

ومن امثلة الوسائل التي تعد اسلحة معلوماتية الاتي :

١. استخدام برامج القنابل المنطقية Logic Bombs

التي تعد بمثابة برنامج ينفذ في لحظة محددة او كل فترة زمنية منتظمة ويتم وصعه في شبكة معلوماتية بهدف تحديد ظروف او حالة مضمون النظام بغية تسهيل تنفيذ العمل غير المشروح ، ومثال ذلك ادراج تعليمات في نظام التشغيل للبحث عن عمل معين يكون محلاً للاعتداء كأن تسعى قنبلة منطقية الى البحث عن حرف (A) في اي سجل تتضمن امراً بالدفع وعندما تكتشفه ، تحرك متتالية منطقية تعمل على ازالة هذا الحرف من السجل.

٢. استخدام برامج الدودة Worm Soflware

وهذه البرامج تعرف بانها تستغل اية فجوات في نظم تشغيل الحاسب الالي لتنتقل من حاسب الى اخر مغطية شبكة باكملها لتحدث اثارها التخريبية للملفات والبرامج ونظم التشغيل وبروتوكولات الاتصال[١٢] .

٣. استخدام فيروسات الحاسب الالي Programms Virus

وهذه تعد من اكثر الوسائل انتشاراً وهي بمثابة (مجموعة من التعليمات المرمزة التي تنتج لنفسها نسخاً مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات ومكونات النظام المنفذ لتقوم في مرحلة محمية بالتحكم في اداء النظام الذي اصابته). وقد عرّفه الركز القومي للحاسب الالي في الولايات المتحدة الامريكية بانه (برنامج مهاجم يصيب انظمة الحاسبات باسلوب يماثل الى حدٍ كبير اسلوب الفيروسات الحيوية التي تصيب الانسان يقوم هذا البرنامج بالتجول في الحاسب الالي باحثاً عن برنامج غير مصاب وعندما يجد واحداً ينتج نسخة من نفسه لتدخلفيه ، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ اوامر الفيروس. ومن اهم خصائصه قدرته الفائقة على الاختفاء والانتشار والاختراق وقدرته على تدمير نظام الحاسب الالي بأكمله [١٣].

٤. هجمات انكار الخدمة : Denial of Service , Dos

وهذه عبارة عن هجمات الكترونية تتم باغراق المواقع بسيل من البيانات غير اللازمة يجري ارسالها ببرامج متخصصة تعمل على نشرها فستؤدي الى بطئ في الخدمات او ازدحاماً مرورياً على هذه المواقع فيصعب بالتالي وصول المستخدمين اليها[١٤].

المبحث الثاني

انواع حرب المعلومات

هناك ثلاثة عناصر اساسية للحرب المعلوماتية وهي (المهاجم) و(المدافع) و(المعلومات ونظمها). وعليه فان هذه الحرب اما أن تكون (هجومية) او أن تكون (دفاعية) ، حيث يتم تحديد طبيعة حرب المعلومات المتتبعة نظراً لما تشمل عليه حرب المعلومات الدفاعية من اعمال مضادة تتصف بصفة الهجوم. ولدراسة ذلك ارتأينا تقسيم هذا المبحث الى مطلبين

المطلب الاول يتناول بالدراسة حرب المعلومات الهجومية اهدافها ووسائلها . والمطلب الثاني يتناول بالدراسة حرب المعلومات الدفاعية اهدافها ووسائلها.

المطلب الاول

حرب المعلومات الهجومية Offensive informdion warfare

أولاً : حرب المعلومات الهجومية

تتضمن حرب المعلومات الهجومية وضع الخطط واتخاذ كافة الاجراءات لاتلاف او تزييف او سرقة او تدمير المعلومات المسجلة او المتداولة على انظمة الحواسيب والاتصالاتالمستخدمة في نظم المعلومات لدى العدو ولمختلف انواع القوات البرية والبحرية والجوية وعلى مختلف المستويات الاستراتيجية والتعبوية والتكتيكية والقيادة والسيطرة وفي كافة المجالات العسكرية والمدنية. ويعتمد انجاح ذلك الانجاز على الاتي :

أ . المعرفة الدقيقة للبنية المعلوماتية لدى العدو.ب . اسلوب تدفق المعلومات خلال قنوات الاتصال لدى العدو .

ج . المعدات المستخدمة لدى العدو والمواصفات الفنية.

د . التطبيقات والبرامج الاساسية المستخدمة في النظم الالية لدى العدو.

هـ . المتابعة المستمرة لاي تحديث لتلك البيانات وملاحظة تطوره[١٥].

وعليه فان الحرب المعلوماتية الهجومية تستهدف معلومات او نظم معلومات محددة عند الطرف المراد مهاجمته ، وذلك لزيادة قيمة تلك المعلومات او نظمها بالنسبة للمهاجم او تقليل قيمتها بالنسبة للمدافع ، او بهما معاً. وذلك لان قيمة المعلومات ونظمها هي المقياس لمقدار

محكّم واستحواذ المهاجم او المدافع بالمعلومات ونظمها على ان الهدف الذي يسعى المهاجم في حربه المعلوماتية لتحقيقه قد تكون اهدافاً مالية كأن يقوم بسرقة وبيع سجلات لحسابات مصرفية وقد تكون تلكالحرب لاهداف سياسية او عسكرية او حتى لمجرد الاثارة واظهار القدرات كما في حالة قراصنة المعلومات.

ان عمليات الحرب المعلوماتية المتعلقة بزيادة قيمة المعلومات ونظمها بالنسبة للمهاجم عدة اشكال ، مناهمها القيام بالتجسس على الهدف لسرقة معلومات سرية بغض النظر عن الاهداف التي قد تكون تجاره بين الشركات او استراتيجية وعسكرية بين دولٍ معينة. ومن تلك العمليات ايضاً التعدي على الملكية الفكرية وقرصنة المعلومات كسرقة البرامج الحاسوبية وتوزيع مواد مكتوبة او مصورة بدون اذن المالك الشرعي ، خاصة وان وجود شبكة الانترنت قد ادى الى توسيع وانتشار مثل تلك العمليات لسهولة النشر والتوزيع على هذه الشبكة[١٦].

اما بالنسبة لعمليات حرب المعلومات المتعلقة بتقليل قيمة المعلومات او نظمها بالنسبة للمدافع فهي (ما أن تكون على صورة التخريب لتلك النظم او على صورة التعطيل لها مثل تعطيل اجهزة الحواسيب وانظمة الاتصالات بكافة انواعها. ومن امثلة ذلك الهجوم الالكتروني الذي استهدف استوني في العام ٢٠٠٧ والذي ادى الى تعطيل المواقع الالكترونية الحكومية والتجارية والمصرفية والاعلامية مسبباً خسائر مادية فادحة ادت الى الاضرار بالبلاد[١٧].

الى جانب ما تقدم تتعدد اصناف المهاجمين في هذه الحرب فقد يكون المهاجم شخصاً يعمل بمفرده ا وان يكون ضمن منظومة تجارية او سياسية او عسكرية ، على ان احداهم اصناف المهاجمين هو من يعمل لدى الجهة التي يراد مهاجمتها لان ذلك يتيح له القدرة على معرفة معلومات حساسة وخطيرة مثال ذلك قيام شخص يشغل مركزاً على قدر من الاهمية في احدى المؤسسات والبنوك له استغلال استخدامه للحاسب الالي للحصول على اية معلومات يرغب بها بغية اختلاس العديد من المبالغ المالية منتهزاً ضعف مراقبة الحاسب الالي لدى مشروعية هذا العمل وعدم قدرته على ذلك في اغلب الأحيان [١٨].

الصنف الثاني للمهاجمين الالكترونيين هم اولئك الذين يعملون على سرقة معلومات مهمة من جهات تجارية او حكومية لا ينتمون اليها لغرض بيعها الى جهات اخرى تهمها تلك المعلومات.

الصنف الثالث يمثله القراصنة او ما يعرف بالهاكرز (hackers) وهؤلاء يعملون عبر الاختراق البرمجي لاجهزة الحاسب الالي فهذه الفئة التي تعد من صنف القراصنة الهواة الى جانب الفئة التي يمثلها المخترقون المحترفون او ما يعرف بـ (الكراكر (Crackers) ، ويتمتعون

بالقدرة على التحكم في برامج الحاسوب وطرق إدارتها واختراقها ومعرفة محتواها ، دون وجه حق وبشكل غير مصرّح به ويكون ذلك اما بصورة مباشرة عن طريق الحصول على كلمة السر او بصورة غير مباشرة عن طريق التقاط الموجات الكهرومغناطيسية المنبعثة من الحاسب الالي اثناء تشغيله وترجمتها[١٩].

الصنف الرابع تمثله الحكومات في بعض الدول التي تسعى من خلال حروب جاسوسية الحصول على معلومات استراتيجية وعسكرية عن الدول الاخرى ومن امثلتها الحروب الجاسوسية بين الولايات المتحدة الامريكية والاتحاد السوفيتي خلال الحرب الباردة. وما تسعى بعض الدول في الوقت الحاضر باستخدام شبكات الاتصال والمعلومات لتحقيق ذات الاهداف بالتجسس والتسلل ثم القيام بتدمير المواقع الالكترونية ، سواء اكانت تلك الصراعات مدفوعة بدوافع سياسية او تنافسية او انها تدور حول الحصول على المعلومات والتاثير في الافكار وشن حرب نفسية واعلامية وتسريب المعلومات ، ومثال الاخير الدور الذي لعبه موقع ويكيليكس في الساحة الدولية[٢٠].

ثانياً: اهداف حرب المعلومات الهجومية ووسائل تحقيقها

تتمثل اهداف هذه الحرب بالاتي :

١. منع تدفق المعلومات بين قادة الخصم ووحداتهم ويمكن تحقيق ذلك الهدف بواحدة او اكثر من الوسائل الاتية :

أ . العمليات الجوية لتدمير مراكز انظمة القيادة والسيطرة.

ب . العمليات الخاصة لقطع خطوط الاتصالات وتخريب محطات الاعادة.

ج . التشويش الالكتروني على اتصالات الخصم.

٢. تشويه معلومات الخصم عن ميدان المعركة ويكون ذلك باحدى الوسائل الاتية :

أ . ادخال اهدافوهمية في رادارات الخصم بواسطة الخداع الالكتروني.

ب . تنفيذ الخداع العسكري في مسرح العمليات ، مثل تحريك بعض عناصر القوة المناطق بعيدة عن الاتجاه الفعلي للعملية وتطبيق اجراءات الاخفاء والتمويه.

ج . اختراق شبكات الحاسب الالي التابعة للخصم وحقنها بمعلومات غير دقيقة[٢١].

اما وسائل تحقيق الاهداف اعلاه فهي كالاتي :

أ . الهجوم الالكتروني (Electronic Attack , EA) ومن امثلته التشويش والخداع الالكتروني والصواريخ المضادة للاشعاع الكهرومغناطيسي.

ب . العمليات الفسلجية (Psychological Operations , Psyops) وهذه العمليات تنفذ ضد الخصم باستخدام وسائل الاعلام المرئية والمسموعة والمقروءة او توزيع المنشورات وهذا يؤدي بالتالي الى زعزعة الثقة لدى الخصم بقدراته وبث الفُرقة بين صفوفه.

ج . التدمير الفعلي المادي (Physical Destruction) ويتم ذلك بالتدمير الفعلي بواسطة الاسلحة الجوية والبرية والبحرية التقليدية او بعمليات القوات الخاصة.

د . الهجمات على شبكات الحاسب الالي (Computer Network – Attack CNA) وهذه تشمل اختراق الشبكات لحقن الحاسبات الالية ببيانات ومعلومات محرّفة لارباك مستخدمي الحاسب الالي او نشر الفيروسات كما اشرنا سابقاً.

وعند المقارنة بين الوسائل الهجومية اعلاه من حيث :

١. تكلفة المعدات والاجهزة اللازمة لتنفيذ العملية المعلوماتية.

٢. مدى توافر المعدات والاجهزة في الاسواق وامكانية الحصول عليها.

٣. درجة الامان بالنسبة لمنفذ العملية المعلوماتية.

٤. صعوبة تنفيذ العملية.

نجد ان افضل تلك الوسائل هي الهجمات على شبكات الحسب الالي على اساس ان الاجهزة والبرمجيات اللازمة لتنفيذها تجارية ومتوافرة في الاسواق باسعار وتكاليف اقل من الوسائل الاخرى الى جانب صعوبة اكتشاف هوية منفذ الهجوم[٢٢].

المطلب الثاني

حرب المعلومات الدفاعية

أولاً : تتمثل هذه الحرب بجميع الوسائل الوقائية المتوافرة للحد من اعمال التخريب التي قد تتعرض لها نظم المعلومات ، والمعلوم أن الوسائل الدفاعية تختلف باختلاف الادوات التخريبية التي تستخدم لشن الهجوم على اجهزة الحاسوب وطبيعة الاضرار التي قد تُحدثها.وعليه فان

الوسائل الدفاعية تمثل بالوقاية والمنع من جهة والتحذير والتنبيه وكشف الاختراقات من جهة اخرى.

أ . المنع والوقاية : وفيها يمنع حدوث المخاطر من البداية وذلك بحماية نظم المعلومات من وصول المهاجمين اليها كاتخاذ اجراءات اخفاء المعلومات (Information Hiding) وتشفيرها (Coding) وكذلك اجراءات التحكم في الدخول الى نظم المعلومات (Access Control).

ب . التحذير والتنبيه : والذي يسعى لتوقع حدوث الهجوم قبل وقوعه في مراحله الاولى.

ج . كشف الاختراقات وكيفية التعامل معها : ويشمل هذا على وسائل تقليدية كاستخدام كاميرات مراقبة للكشف عن الدخول غير المصرّح به للمبنى الذي يضّم نظم المعلومات المطلوب حمايتها الى جانب وسائل تقنية جاسوسية تتمثل في برامج واجهزة تقوم بمراقبة العمليات التي تنفذها نظم المعلومات لكشف عن العمليات غير المصرّح بها حين تعتبر مؤشراً لاختراقات خطيرة على تلك النظم.

اما التعامل مع الاختراقات فانها تتضمن الاليات اللازمة للتعامل مع الاختراقات بعد حدوثها مثال ذلك كيفية اعادة النظم الى وضعها الطبيعي وتجتمع الادلة والبراهين التي يمكن من خلالها معرفة هوية المخترق ومقاضاته وتوثيق الحادث لتجنب تكراره مستقبلاً[٢٣].

ثانياً : وعليه يمكن اجمال وسائل الحرب المعلوماتية الدفاعية بالاتي :

١. الحماية الالكترونية Electronic Protection , E P

وهذه الوسيلة بدورها ذات شقين هما :

الاول : هو اجراءات حماية الكترونية وقائية تطبق في السلم والحرب لحرمان الخصم من التقاط البث الصادر من اجهزة الاتصالات والرادارات التابعة للمدافع.

والثاني : هو اجراءات الحماية الالكترونية العلاجية التي تُطبق في حال تعرض الاجهزة للهجوم الالكتروني لتجاوز اثاره او تقليلها.

٢. الاجراءات الامنية Security Procedures

وهذه تشتمل على امن المعلومات الذي يُعد بمثابة تدابير لحماية سرية وسلامة المعلومات من الاخطار الداخلية والخارجية الى جانب مكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة بالاضافة الى امن الحاسبات وامن الوثائق وامن الاتصالات ولكنها تهدف الى منع وصول الخصم الى معلومات المدافع وانظمته المعلوماتية.

ومن وسائل امن المعلومات الشائعة :

ا . الوسائل المتعلقة بالتعريف بالشخص المستخدم وموثوقية الاستخدام ومشروعيته Identification and authenticationوهذه بدورها ضمان استخدام النظام او الشبكة من قبل الشخص المخول بالاستخدام وتضم هذه الطائفة كلمات السر بانواعها والبطاقات الذكية المستخدمة للتعريف.

ب . الوسائل التي تهدف الى منع افشاء المعلومات لغير المخولين بذلك وذلك لتحقيق سرية المعلومات Data and Message Confidentialityويعد التشفير احد هذه الوسائل.

فتشفير وترميز المعطيات والحلقات يعد وسيلة مهمة لتحقيق وظائف امن المعلومات المتمثلة بالسرية والتكاملية وتوفير المعلومات وتعد هذه الوسيلة علىجانب من الاهمية في بيئة الاعمال والتجارة الالكترونية والرسائل الالكترونية وجميع البيانات التي يتم تداولها بهذه الوسائط.

جـ . الوسائل التي تهدف الى حماية سلامة المحتوى Data and message integrity وهذه الوسائل يُناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخوّلة بذلك.

د . وسائل مراقبة الاستخدام وتتبع سجلات النفاذ او الاداء Logging and Monitoringوهذه التقنية تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين ، وتشتمل على انواع البرمجيات الالكترونية التي تحدد الاستخدام[٢٤].

٣. العمليات النفسية المضادة Counter – Psyops

والغرض منها هو اكتشاف مثل تلك العمليات التي يمارسها المهاجم والعمل على مواجهتها باستخدام وسائل الاعلام المختلفة والعمل على رفع المعلومات ومقاومة الاشاعات.

٤. الخداع العسكري Military Deception

وهذه تشتمل على عمليات الاخفاء والتمويه وتحريك بعض الوحدات في اتجاهات واقعية ولكنها بعيدة عن الاتجاه الفعلي للهجوم ، بالاضافة الى قيام القادة السياسيين والعسكريين بالتصريح والادلاء بمعلومات غير صحيحة عن الوضع العسكري[٢٥].

هذا ومن الجدير بالاشارة اليه ان لحرب المعلومات سبعة اقسام كما اشار لذلك الدكتور (مارتن ليبكي) من جامعة الدفاع القومي الامريكي وهي كالاتي :

١. الحرب الالكترونية.

٢. حرب القيادة والسيطرة.

٣. حرب قراصنة المعلومات.

٤. الحرب الاستخبارية.

٥. حرب العمليات النفسية.

٦. حرب المعلومات الاقتصادية.

٧. حرب المعلومات الافتراضية[٢٦].

الخاتمة

على الرغم من ان هناك جدلاً واسعاً عن وجود او عدم وجود ثورة في الشؤون العسكرية ، فان من الصعب انكار أن وسائل الحرب في القرن الحادي والعشرين تختلف بصورة جذرية عن الوسائل التي كان يتسم بها القرن العشرين.

في بداية القرن الجديد ، وبعد احداث الحادي عشر من ايلول من عام ٢٠٠١ ، ستكون (حرب المعلومات) احدى اهم الوسائل القتالية التي ستتحدى المذاهب القائمة عن شن الحرب واستخدام القوة ، وستتطلب مراجعة لمفهوم ساحة المعركة التي اضحت مختلفة عن ساحة الحرب التقليدية بحدودها المادية ، على اسا ان شبكات الاتصال الرقمية وحيّزها ،اصبحت تمثل ساحات للقتال بالاسلحة التكنولوجية المتمثلة بالفيروسات وغيرها وهذا يعني توسع القتال ووسائله وعليه فان قدرة كل دولة على الحفاظ على اتصالاتها وقيادتها وسيطرتها وقدراتها الحاسوبية ضد الهجمات من قبل الافراد او الجماعات الارهابية او عصابات الجريمة المنظمة او من الدول ، لم تعد مؤكدة في ظل التطور التكنولوجي المعلوماتي ، فتنوع الاهداف وتغيّر طبيعة الدمار الذي ينجم عن مثل تلك الهجمات وامكانية الوصول للاهداف دون الحاجة الى التواجد في الاقليم الذي تقوم فيه الى جانب استخدام المهاجم لتكنولوجيا التجهيل او الحجب مما جعله مجهول الهوية[٢٧].

جميع الخصائص هذه قد يؤدي الى تحديات مختلفة لمفاهيم ومبادئ تعد ثابتة ، وبخاصة في نطاق القانون الدولي مما يتعلق بمبدأ السيادة ، ومدى شرعية لجوء الاطراف الى استخدام القوة او استخدام حق الدفاع عن النفس في مواجهة تلك الهجمات وما يستتبعه مما يتعلق بمبدأ مسؤولية الدول والولاية القضائية ،وان كانت بعض الول قد عملت على سن تشريعات تتعلق بالجرائم الالكترونية ومنها الاتفاقية الاوربية لمكافحة جرائم الانترنت (اتفاقية بودابست ٢٠٠١) وكذلك الاتفاقية الامريكية المتعلقة بجرائم الحاسوب الانترنت لعام ١٩٩٩ ، وعلى صعيد الدول العربية فقد قامت المملكة العربية السعودية في عام ٢٠٠٧ بوضع نظام مكافحة جرائم المعلوماتية والتعاملات الالكترونية وفي الامارات صدر القانون الاتحادي لعام ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات.

الا ان الاستخدام الواسع للوسائل والشبكات الالكترونية من قبل الدول لاستهداف دولٍ اخرى ومنها ما وقع في استونيا عام ٢٠٠٧ وفي جورجيا عام ٢٠٠٨ وفي ايران عام ٢٠١٠ ، يعد تهديداً للامن الدولي باكمله مما يستوجب ويستدعي التعاون الدولي من اجل وضع استراتيجيات

تكون قابلة للتطبيق والتنفيذ على الصعيد العالمي الى جانب التشريعات القائمة على الصعيدين الوطني والاقليمي.

الهوامش

(١) قيادة الاركان المشتركة ، قاموس وزارة الدفاع للمصطلحات العسكرية وما يتعلق بها ، طبعة مشتركة (1 . , 0212) نيسان 2001 ، ص203.

(٢) Michael N. Schmitt , Wired Warfare : Computer Network Attack and Jus in Bello , International Review of the Red Cross , No. 869 , 2002 , p365.

(٣) انظر : جمال محمد غيطاس ، الحرب وتكنولوجيا المعلومات ، القاهرة ، دار نهضة مصر ، الطبعة الاولى، ٢٠٠٦ ، ص٣ . ٦.

(٤) قيادة الاركان المشتركة ، الاستراتيجية العسكرية القومية ، 1997.

موجود على الرابط الالكتروني : http : www. Dtic . mil / jcs / nms / Strategy. == Htm , (1997).

== Richard W. AL drich , The International Legal Implications of Information Warfare , Institute National Security Studies , U.S force Academy , Colorado , April , 1996 , p42.

(٥) انظر : دليل القوات الجوية الامريكية لاستهداف المخابرات ، كتيب القوات الجوية – 210 14 ، شباط 1998 ، الفقرة 11.43.

(٦) لقد كانت اول تجربة لمراقبة الارض من الفضاء الخارجي ، حين قام الاتحاد السوفيتي باطلا قاول مركبة فضاء (فوستوكVostok) عام ١٩٦٠ حاملة رائد الفضاء (يوري جاجارين) الذي عاد الى الارض بعد ساعة وثمانية واربعون دقيقة. ومنذ تلكالرحلة الطفرة التكنولوجية الهائلة في انواع المستشعرات التي تركب على الاجسام الفضائية سواء الماهولة منها او غير الماهولة. انظر : بن حمودة ليلى ، الاستخدام السلمي للفاضء الخارجي ، المؤسسة الجامعية للدراسات والنشر والتوزيع ، الطبعة لاولى ، بيروت ، لبنان ٢٠٠٨ ، ٢٣٢.

(٧) يمكن تقسيم الطائرات بدون طيار بحسب المهمات التي تضطلع بها الى ثلاثة انواع اساسية هي / الطائرات بلا طيار المتخصصة في مجال المراقبة والتي تكشل الجزء الاكبر من هذه

الطائرات والطائرات بلا طيار المزودة بالصواريخ والطائرات بلا طيار مزدوجة الاستخدام والتي يمكن استخدامها للغرضين السابقين معاً. انظر : د. طارق المجذوب ، الطائرات بلا طيار كوسيلة حرب ، مجلة الدفاع الوطني ، ٢٠١٢ ، ١ . ٥.

(٨) انظر : يونس عرب ، امن المعلومات ماهيتها وعناصرها استراتيجيتها ، ، ، ص٣٢ . ٣٦.

(٩) انظر : جمال محمد عنطاس ، المصدر السابق ، ص٥ . ٦.

(١٠) لقد تنبه المشرع الفرنسي لاهمية هذا الامر فاصدر القانون بالمعلوماتية والبطاقات والحريات في عام ١٩٧٨ والمعدل عام ١٩٨٨. انظر : محمد عبدالله ابو بكر سلامة ، جرائم الكمبيوتر والانترنت ، منشأة المعارف ، الاسكندرية ، ٢٠٠٦ ، ص١٠٣ . ١٠٨.

(١١) Lawrence T. Greenbery , Kevin J. SooHoo , Seymour E. Goodman , Information Warfare and International Law , National Defence University Press , 1998 , P 14– 20.

(١٢) محمد امين الرومي ، جرائم الكمبيوتر والانترنت ، دار المطبوعات الجامعية ، الاسكندرية ، ٢٠٠٣ ، ص٨٥.

(١٣) انظر : محمد عبدالله ابو بكر سلامة ، المصدر السابق ، ص١٥٤ . ١٦٥. وانظر : جانكارلو أ. باراليتا وغيرهم ، النزاع السيبراني والاستقرار الجيوسيبراني ، الاتحاد الدولي للاتصالات ، ٢٠١١ ، ص٤٨ . ٥٠.

(١٤) Ian Trayna , Web Attackers Vsed a Million Computers < Says Estonia , Gardian (London) , 18 May , 2007.

(١٥) انظر :احمد مغربي ، الهجوم على الشبكات وقوانين الحرب ، ٢٠١٢ ، ص٣ . ٤.

(١٦) انظر :جمال محمد غيطاس ، المصدر السابق ، ص٨.

(١٧) انظر : علي حسن باكير ، الحروب الالكترونية في القرن ٢١ ، ص١ . ٣.

Amir Lupovici , Cyber Warfare and Deterrence : Trends and Challenges in Research , Military and Strategic Affairs , Vol.3 , No.3 , December 2011 ,P 49 – 55.

(١٨) انظر : عبدالله ابو بكر سلامة ، المصدر السابق ، ص١٧٠.

(١٩) د. هشام محمد فريد رستم قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الالات الحديثة ، اسيوط ، ١٩٩٤ ، ص١٠٧. خالد وليد محمود ، الهجمات عبر الانترنت ، ساحة الصراع الالكتروني الجديدة ، المركز العربي للابحاث ودراسة السياسات ، ٢٠١٣ ، ص٧ . ١٠.

(٢٠) نوران شفيق علي ، فواعل افتراضية ، المواجهات الالكترونية بين القوى السياسية بعد الثورات العربية ، مجلة السياسة الدولية ، حزيران ٢٠١٣. موجود على الرابط الالكتروني :

http://www.siyassa.org.eg/News Content/2/106/3137.

عادل عبد الصادق ، موقع ويكيليكس وتحدي عالم الاستخبارات الامريكي ، مركز الاهرام للدراسات السياسية والاستراتيجية ، ٢٠١٠ ، ص٤.

(٢١) سمير محمد شحاته، القوة في العلاقات الدولية ، نمط جديد وتحديات مختلفة ، موجود على الرابط الالكتروني .www/ digital.alahram.org ،

(٢٢) Heather Harrison Dinniss , Cyber warfare and the Laws of War , Camberidge University Press , 2012 , P 4-10.

القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ، المؤتمر الحادي والثلاثون للصليب الاحمر والهلال الاحمر ، اللجنة الدولية للصليب الاحمر ، جنيف ، تشرين الاول ، ٢٠١١ ، ص٤٤ . ٤٦.

(٢٣) عادل عبد الصادق ، القوة الالكترونية اسلحة الانتشار الشامل في عصر الفضاء الالكتروني ، مجلة السياسة الدولية ، ص ٦

(٢٤) يوسن عرب ، امن المعلومات ، ماهيتها وعناصرها وإستراتيجيتها ، المصدر السابق ، ص٤٧ . ٥٠.

(٢٥) Clay Wilson , Information Warfare and Cyberwcrl : Capabilties and related Policy issues , Congressional Research service , the Libray Congress , July 19 , 2004 , P2 – 7.

(٢٦) Hathaway , Crootof , The Law oj Cyber – Ahack , California law Review , 2012 , P4.

د. عبد الرحمن عبد العزيز المنيف ، الحرب الالكترونية ، الحرب القادمة ،ص١٠.

(٢٧)هذه التقنيات تجعل بمقدور المستعمل القيام بحذف اية مرجعية من رسائله تسمح بمعرفة صاحبها وبالتالي يتمكن من نقل محتويات كانت تعرض صاحبها للملاحقة القضائية في السابق. ا وان يقوم بتغيير المعطيات بهدف اخفاء محتواها والعمل على ضمان مرور ذلك التغيير دون ملاحظته ودون القيام بمنع الاستعمال غير المصرح به من قبل الجهات المختصة لانه يخالف التشريعات القائمة (الاسرار التجارية). د. محمد سعادي ، السيادة الرقمية ، مجل الفقه والقانون ، العدد الخامس ، آذار ٢٠١٣ ، ص٦٧.