الفصل الخامس عشر

الإرهاب الإلكتروني وأسلحة الطاقة الموجهة
Electronic Terrorism and Directed Energy Weapons

المقدمة

تتراوح لائحة الأسلحة المتاحة للإرهابيين من طائرات الركوب إلى الأجهزة الذرية لتشمل جميع الأسلحة الكيميائية والبيولوجية التي طورّت خلال المائة سنة الماضية ويضاف إلى هذه اللائحة التهديد المتزايد من قبل أسلحة شبكة الإنترنت والإرهاب الإلكتروني والتي يمكن وصفها بأسلحة التشويش الشاملة، بإحداث ضرر كبير على مستوى الأنظمة الإلكترونية المحلية الإلكتروني. سوف يستعرض هذا الفصل المبادئ الأساسية وتقنيات الأسلحة الإلكترونية والإرهاب الإلكتروني كونها قد تؤثر على نظام الخدمات الطبية الإسعافية. يجب التأكيد على أن هذا الفصل غير حصري بل يقصد فقط توضيح كيف يمكن للقاعدة التقنية في العالم ونظام الخدمات الطبية الإسعافية على وجه الخصوص أن يكون عرضة إلى مختلف أنواع الهجوم.

الإرهاب، الكمبيوترات، والإنترنت
Terrorism, Computers, and Internet

يمكن لأية آلة موصولة بالإنترنت أن تقوم بمهمة طابعة، أو محطة إذاعية، أو مكان تجمع. ينبغي على المراقب النبيه أن يلاحظ أن غالبية المنظمات الأجنبية والتي

obeikandl.com

تعتبرها وزارة الخارجية الأمريكية منظمات إرهابية لديها موقع رسمي على الإنترنت.[١] مع ظهور شبكة الإنترنت أصبح بإمكان الجماعات الإرهابية نشر معلوماتها دون أن تستطيع وسائل الإعلام التأثير عليها أو أن تطالها أجهزة الرقابة الحكومية. ويجب أن تطرح الجماعات الإرهابية هذه المعلومات بشكل سهل وسلس بحيث لا يكون لها وقع مفاجئ أو مثير للدهشة وبذلك تستطيع هذه المنظمات أن تستخدم الإنترنت في نشر الإنجيل والتعليمات والدعايات والخطط لكل من الأجهزة والهجمات. ولسوء الحظ، فقد تم تجاهل الاستخدام الإرهابي الفعلي للكمبيوترات والشبكات وأنظمة المعلومات والإنترنت بشكل كبير لصالح السيطرة على عناوين الهجوم الإرهابي عبر الإنترنت ومن هنا تأتي حقيقة ضعفنا التي تقشعر لها الأبدان وتستدعي إعادة النظر فيها بشكل أكبر. لا يوجد تعريف واضح ومفهوم ومقبول على نطاق واسع للإرهاب عبر الإنترنت. وقد طبق المفهوم الازدرائي للإرهاب بشكل خاطئ على حالات سوء استخدام الكمبيوتر ومثال ذلك أن تشمل قائمة البريد الإلكتروني على إصدارات روتينية لمواد إباحية للأطفال على أنها حوادث إرهابية. بالتأكيد، تعتبر هذه المواد جنائية ومنحرفة وعملاً إرهابياً. إن تعبير " الإرهاب " يمكن أن يعرف في قانون عام واحد على أنه: عنفٌ متعمد بدوافع سياسية يُرتكب ضد أهداف غير قتالية من قبل جماعات شبه قومية أو عملاء سريين والمقصود منه عادة التأثير على الجمهور.[٢]

ما مدى تعرضنا للهجوم الإلكتروني عبر الإنترنت؟

نحن فريسة سهلة لهذا النوع من الهجوم وذلك لسببين: الأول، أن التطور التقني المتنامي عند الإرهابيين لا يشمل فقط أسلحة الدمار الشامل والإصابات بل يشمل أيضاً تطوراً في استخدام الكمبيوترات. الثاني، أن أنظمتنا التقنية والاقتصادية أصبحت أكثر عرضة للهجمات في أوقات محددة بدقة مع زيادة اعتمادنا على الكمبيوترات. إن البنية التحتية الرئيسية للولايات المتحدة بما فيها الطاقة الكهربائية،

الاتصالات، الرعاية الصحية، النقل، المياه، والإنترنت كلها عرضة للهجوم الإلكتروني عبر الإنترنت. إن أنظمة السيطرة والاتصالات والإرسال كلها على اتصال بالإنترنت، ولذلك فهي مهددة لأن تكون عرضة للاختراق. ولا يشمل هذا التأثير المحتمل للهجوم عبر الإنترنت أنظمة المال والدفاع الوطني. بينما يمكن للهجوم أن يؤثر على عمليات منظومة الخدمات الطبية الإسعافية وذلك عن طريق ثلاثة سبل هي: الهجوم الفيروسي، الهجوم بطريقة رفض الخدمة، والهجوم النبضي الكهرومغناطيسي.

الفيروسات والديدان Viruses and Worms

يطلق اسم فيروسات عادة على برامج الكمبيوترات الخبيثة، وذلك لأنها تحمل إلى حد ما بعض صفات الفيروسات البيولوجية. وعلى عكس الخلية، فإن الفيروس البيولوجي لا يمكنه التكاثر لوحده بل يتطلب ذلك توفر خلية مضيفة وظيفية. وبشكل مشابه، يتطلب تضاعف فيروس الكمبيوتر جهازاً مضيفاً وظيفياً. علاوة على ذلك يمكن للفيروس أن يعبر من كمبيوتر إلى آخر كما يعبر الفيروس البيولوجي من شخص إلى آخر. توجد مواضع تشابه أخرى بينهما. الفيروس البيولوجي هو جزء من البروتين النووي DNA الموجود ضمن محفظة حامية. يقوم فيروس الكمبيوتر بالارتباط مع برنامج، ملف، أو بريد إلكتروني حتى يتمكن من دخول الكمبيوتر. وفي كثير من الأحيان يجب عليه أن يخفي نفسه من البرامج المضادة للفيروسات حيث يحيط نفسه بحزمة غير ضارة كما يفعل نظيره البيولوجي. الناس هم من يخلق فيروسات الكمبيوتر. يجب على الشخص أن يكتب رمز الفيروس ومن ثم يجربه ليتأكد من أنه يمكن أن ينتشر بالشكل الذي صمم عليه ويؤدي وظيفته بالشكل المطلوب. يعتبر الكمبيوتر الذي يحمل نسخة فعّالة من فيروس على قرصه الصلب " مصاباً " infected وتعتمد طريقة تفعيل الفيروس على نموذج الفيروس (الرمز). تصبح بعض الفيروسات فعَّالة إذا فتح

المستخدم ملفاً مصاباً، بينما تحتاج فيروسات أخرى أن يقوم المستخدم بإجراءات خاصة لتفعيلها. تم كشف فيروسات الكمبيوتر التقليدية عام ١٩٨٠م وخلال هذا العقد انتشر استخدام الكمبيوترات بشكل واسع بدءاً من المواقع المركزية الكبيرة إلى الأعمال الصغيرة والبيوت وذلك نتيجة لتوفر الكمبيوترات الشخصية الصغيرة، وتعتبر فيروسات الحصان الجامح Trojan horse أول الفيروسات المكتشفة. الحصان الجامح ببساطة، برنامج كمبيوتر خبيث يدعي القيام بشيء ما مثل (لعبة أو أداة مساعدة) لكنه بالواقع يعمل شيئاً آخر كأن يقوم بمسح قرصك الصلب. إن برنامج فيروس الحصان الجامح لا يمكنه القيام بالنسخ المتماثل بشكل تلقائي. مثال آخر للفيروسات المكتشفة باكراً فيروس قطاع التشغيل boot sector virus. قطاع التشغيل عبارة عن برنامج صغير يقوم بتهيئة الكمبيوتر وعملية تحميل نظام التشغيل- " تحضيره في الذاكرة booting ". ومع وضع الرمز الفيروسي في قطاع التشغيل، يكون الفيروس قد ضمن تحميله في الذاكرة فوراً ليكون قادراً على العمل عند تشغيل الكمبيوتر. ويعمل هذا الفيروس على إصابة قطاع التشغيل لأي قرص مرن يدخل الجهاز المصاب. لم نعد نجد هذا النوع من الفيروسات لأن صنّاع أنظمة التشغيل والبرامج المضادة للفيروسات قاموا بحماية قطاع التشغيل، ويستخدم معظم الناس القرص الصلب في عملية التشغيل، ناهيك عن أن معظم البرامج تُحمَّل من أقراص مدمجة CDs والتي تعتبر أقل عرضة لتعديلات قطاع التشغيل. عندما يصبح الفيروس فعَّالاً على جهاز الكمبيوتر، يصبح بإمكانه أن ينسخ نفسه إلى ملفات، أقراص، وبرامج يستخدمها الكمبيوتر (سواء تم الوصول إليها آلياً أوعن طريق مستخدم الكمبيوتر). يكمن الاختلاف الكبير بين فيروسات الكمبيوتر والبرامج الأخرى في أن فيروسات الكمبيوتر لها تصميم خاص يمكنها أن تنسخ نفسها وعندما يجري التخلص من برنامج الفيروس، يقوم الفيروس بفحص الأقراص الصلبة باحثاً عن برامج أخرى" معرَّضة للإصابة " على القرص الصلب، وعندما يجد برنامجاً

كهذا، يقوم الفيروس بتعديله عن طريق إضافة رمز فيروسي له أو باستبدال الملف أو البرنامج برمز الفيروس الخاص به وعندما يتم إنجاز ذلك، يمكن للفيروس نسخ نفسه وبذلك نحصل على عدة ملفات مصابة. وكلما قام المستخدم بفتح ملفات مصابة، يكون لدى الفيروس فرصة للتكاثر عن طريق الارتباط بملفات أخرى، وهكذا تتوالى الدائرة. ويحصل هذا التضاعف دون علم مستخدم الكمبيوتر (أحياناً يكون البرنامج المصاب برنامج نظام لا يمكن للمستخدم السيطرة عليه). يمكن أن تحوي الروابط التي تأتي على شكل ملفات نظام مثل ملفات المايكرو سوفت وورد (DOC)، أو جداول البيانات إكسل (XLS)، وصور (GIF.JPG)، على فيروسات. كما يمكن تنفيذ البرنامج الذي يحوي ملحقاً مثل EXE,COM,VBS مما قد يولّد برنامجاً فيروسياً يمكنه إلحاق الضرر بالكمبيوتر على أي مستوى. تستطيع الكثير من الفيروسات أن تموه نفسها عن طريق مضاعفة ملحق اسم الملف (مثال ذلك، STUFF.GIF.VBS). يحمل الفيروس عادة حمولة payload أوعملاً إضافياً يقوم به بالإضافة إلى مضاعفة نفسه ويتراوح هذا من عمل تافه مزعج إلى عمل مدمر. تشمل بعض الأعمال غير المدمرة وغير المزعجة تسجيل الدخول إلى البرامج التي تقوم بتسجيل كل ضغطة زر، البرامج التي تقوم بإرسال البريد الإلكتروني إلى كل العناوين الموجودة على الكمبيوتر بشكل تلقائي، والبرامج التي تفتح قنوات تسمح بدخول العناصر الغريبة تقوم بفحص واستخدام كمبيوترك الخاص. ولو كانت حمولة الفيروس مصممة بشكل جيد، فإنه قد لا يكون باستطاعة المستخدم معرفة أن كمبيوتره مصاب. وقد أوضحت الهجمات السابقة قدرة البرنامج الفيروسي على اكتساب بيانات وأرقام سرية ومن ثمَّ إرسال هذه المعلومات بالبريد الإلكتروني إلى شخص معين. يمكن استخدام أجهزة الكمبيوترات العامة والتجارية (غير المؤمنة) والرسمية وبعض الأنظمة المؤمنة كأجهزة تحكم في جمع المعلومات الاستخباراتية. وعادة ما يكون تحديد موقع البرنامج المتسبب صعباً لأن

العديد من البرامج ذوات مفاتيح تسجيل جرى إخفاؤها على شكل ملفات ومجلدات نظام أساسية. "الدودة" worm ببساطة عبارة عن فيروسات لها القدرة على نسخ نفسها من جهاز كمبيوتر إلى آخر وهذه النسخة تصيب شبكة الكمبيوتر المتاحة من خلال نفس الخلل الأمني. ومع استخدام الشبكة والإنترنت، يمكن للديدان أن تصيب الأجهزة الأخرى بسرعة لا تصدَّق. يمكن أن تتواجد فيروسات الكمبيوتر الحديثة في البرامج المتاحة على الأقراص المرنة والمضغوطة كما أنها يمكنها الاختباء ضمن أنواع مختلفة من روابط البريد الإلكتروني والمواد المحملة من الإنترنت. لماذا يعتبر هذا مهماً بالنسبة للخدمات الطبية الإسعافية ؟ وما الضرر المحتمل أن يأتي من الفيروس الذي ينتشر بالبريد الإلكتروني أكثر من أن يفكك ذلك البريد الإلكتروني ؟ بعض الإجابات عن هذه الأسئلة أصبحت جلية بعد استعراض الفيروسات الحديثة والديدان.

أحداث ذات صلة بالإرهاب الإلكتروني

جوجو جيانغ

لمدة أكثر من عام، قام هذا الشخص والذي يجهله الناس باستخدام محطات الإنترنت لدى مستودعات كينكوز في نيويورك، كان جوجو جيانغ يسجل كل ما يطبعونه، ويولي اهتماماً خاصاً لأرقامهم السرية. ويقوم بشكل سري، في العديد من مستودعات كينكوز، بعمليات تحميل البرامج التي تسجل ضغطات المفاتيح الشخصية. لقد استولى على أكثر من ٤٥٠ من أسماء المستخدمين مع أرقامهم السرية، واستخدمها في الدخول وفتح الحسابات البنكية على الإنترنت.[٣]

تعتبر "دودة الرمز الأحمر" Code Red واحدة من أحدث الفيروسات والديدان المدمرة (وحالياً لها أنواع متعددة) وكان أول ظهور لها في تموز ٢٠٠١م وقد تسبب

بإصابة ٣٠٠٠٠٠ كمبيوتر تقريباً في الولايات المتحدة. ويستغل هذا النوع من الديدان الفجوة في خوادم الويب IIS لمايكروسوفت ولا تزال السلطات تجهل من أين نشأت هذه الدودة ومن كان محررها. وقد جرى تفعيل هذه الدودة اعتماداً على التاريخ، فمن اليوم ١ إلى ١٩ من الشهر تنتشر الدودة، ومن اليوم ٢٠ إلى ٢٧ تقوم الدودة بشن هجوم ضد الموقع المحدد، ومن اليوم ٢٧ إلى نهاية الشهر تنام الدودة في الكمبيوتر.[٤] وقد فتحت بعض الأشكال من الدودة منافذ وصول سرية (أبواب خلفية back doors) في أنظمة التشغيل مما يسمح بحدوث تدخلات أخرى. يعتبر مفهوم منافذ الوصول السرية أمراً هاماً. تسمح هذه المواقع السرية للدخول للمبرمج الخبيث من الوصول وحتى السيطرة على البرامج التي هي قيد التشغيل في الكمبيوتر المصاب. وهذا المنفذ يمكن الحصول عليه عن طريق فيروس يقوم بإصابة البرامج التي هي جزء من (مساعدة بعيدة) الخدمات في بعض أنظمة التشغيل، أو أن يقوم المصمم أو المبرمج (الساخط أو المشغل تحت تعليمات) بإنشاء منفذ الوصول ضمن برنامج معين. ومع أن مايكروسوفت قدمت تصحيحاً لدودة الرمز الأحمر، لكن العديد من إداريي الأنظمة لم يطبقوا هذا التصحيح في أنظمتهم لتبقى هذه الكمبيوترات عرضة لهذا الفيروس. قد تحمل التدخلات الأحدث لهذا الفيروس هدفا أكثر خبثاً، ففي صيف ٢٠٠١م، لاحظ منسق موقع ويب في كاليفورنيا نموذجاً مثيراً للشك من التدخلات. ومع التحريات التي قام بها مكتب التحقيقات الفيدرالي تبين أن العديد من مدن الولايات المتحدة الأمريكية تعرضت لنفس التدخلات. وقد نشأت هذه التحقيقات من الشرق الأوسط وجنوب آسيا، حيث كان الغزاة يبحثون عن معلومات عن المدن، المرافق العامة، المكاتب الحكومية وأنظمة الطوارئ. أخذت هذه المعلومة أهمية جديدة بعد استيلاء نشطاء القاعدة على العديد من الكمبيوترات بعد هجمات ١١ أيلول، واكتشف المسؤولون وجود نمط واسع النطاق لمراقبة البنية التحتية للولايات المتحدة على هذه الكمبيوترات.[٥]

وبعد أسبوع من أحداث ١١ أيلول ظهرت دودة نيمدا Nimda worm التي هاجمت القطاع المالي. وهي دودة يمكن أن تضاعف نفسها بعدة طرق: يمكن أن تقوم بإصابة برامج البريد الإلكتروني، وتطبع نفسها في خوادم الكمبيوتر، أو أن تقوم بإصابة المستخدمين الذين يحمِّلون صفحات مصابة من خوادم الويب المصابة. لقد استطاعت نيمدا أن تؤثر على ملايين الكمبيوترات عن طريق الزحف عبر الإنترنت. يمكن لدودة نيمدا أن تضاعف نفسها بشكل أسرع من دودة الرمز الأحمر لتسبب خسائر تقدر بمليارات الدولارات.[٦] ظهرت دودة سلامر Slammer worm على الساحة في ٢٥ كانون ثاني من عام ٢٠٠٣م واستغلت الضعف في الخوادم التي تزود المستخدمين بصفحات الويب. لقد كانت الأسرع في القيام بالهجوم الإلكتروني عبر التاريخ، حيث تتضاعفت الإصابة بهذه الدودة مرة كل ٨,٥ ثانية وتحدث ٩٠٪ من الضرر الذي تسببه في أول ١٠ دقائق من تحررها. لقد تسببت هذه الدودة بإحداث عجز في أجزاء من الإنترنت في كوريا واليابان، كما عطَّلت الخدمة الهاتفية في فنلندا، وأبطأت بوضوح أنظمة حجوزات شركات الطيران وشبكات بطاقات الائتمان والصرف الآلي في الولايات المتحدة.[٧] يمكن لهذه الدودة أن يكون لها تأثير مدمر وضار أكثر لو تمت برمجتها بالأسلوب المناسب كما يمكنها التأثير على أنظمة الاتصالات الهاتفية (بما فيها بعض الروابط الإذاعية) في المدينة أو حتى منطقة أكبر من الدولة ومع أنه من غير المرجح أن يؤثر فيروس الإنترنت مثل دودة سلامر على أنظمة السيطرة والتحكم بشكل مباشر، لكن قد يحدث فقدان للخدمة في نقاط التحكم في أنظمة توزيع المياه ونقاط تحويل السكك الحديدية وشبكات الكهرباء والنباتات الكيميائية وأنظمة الهاتف مما يسبب فشلاً غير تدميري كبيراً. وبعد رسم خرائط نقاط الوصول الآنفة الذكر، يقوم الإرهابيون باستهداف نقاط ضعف محددة ومضايقتها.

الآثار والتداعيات المترتبة

يمكن تصميم لأيٍّ من الفيروسات والديدان الحديثة أن تصميمها من جديد بهدف القيام بالتدمير أو على الأقل إحداث الشلل في نظام١- ١- ٩ الموجود في الولايات المتحدة ليشمل: أنظمة الطاقة الكهربائية، أنظمة النقل، أنظمة الاتصالات، أنظمة إمدادات المياه وقد يشمل أنظمتنا الدفاعية.

ماذا بإمكانك أن تفعل للمساعدة؟

أحد أفضل الأشياء التي يمكنك فعلها أن تحمِّل برنامج مضاد للفيروسات جيد على جهاز كمبيوترك وأن تقوم بتحديثه بشكل دوري. قم بإعداد جدول تحديث نظام التشغيل وقم بتشغيل برنامج المسح الفيروسي، وإذا تم العثور على فيروس قم بحذفه. يصمم كل فيروس من أجل برنامج تشغيل معين، فإذا كنت تعمل على عدة أنواع من نوافذ المايكروسوفت (٩٨ – ٢٠٠٠ – XP) فإن الفيروس المصمم من أجل نافذة يونيكس لن يستطيع التأثير على كمبيوترك. صممت بعض الفيروسات لاستغلال نقاط الضعف المعروفة في البرامج الشعبية. إذا لم يكن برنامج بريدك الإلكتروني هو برنامج " آفاق المايكروسوفت " Microsoft outlook فإن الفيروسات التي تصيب هذا البرنامج لن تسبب مشاكل لك.

- هل تمَّ إعداد برنامج الحماية من الفيروسات من أجل مسح الوثائق قبل فتحها.

- لا تقم بفتح أي ملف قد تمَّ إرساله لك إلا إذا كنت تعرف مصدره وتثق به. وبحال قمت بفتح الملف وكان يحوي فيروساً أو دودة مؤذية فإن نظام كمبيوترك سوف يصاب وستنتقل هذه الإصابة لأي شخص ترسل له هذا البريد الإلكتروني.

- لا تقم بإجراء النقر مرتين على الرابط الذي يصلك من البريد الإلكتروني إلا إذا كنت تعرف مصدره وتتوقعه، ولا تظن ببساطة أنك تفتح صورة.

- لا تستخدم الوحدات الكلية في تطبيقات المايكروسوفت إلا إذا كنت تعرف مصدرها، وهي عبارة عن مركبات عامة "Macros "لنقل الفيروسات إلى أنظمة المياكروسوفت.

- تأكد من أن مدير إدارتك لديه خطة احتياطية قوية ولديه نسخة جاهزة ومحدَّثة لاستعادة النظام بحيث يستطيع استعادة نظامك التشغيلي في الحالات الطارئة.

- بالنسبة للذين يعملون مع أنظمة التشغيل الأساسية مثل مراكز الإرسال، يجب عليهم إجراء تقييم خبير لأجهزتهم للتحري وجود أبواب خلفية مخفية تسمح بالتدخلات. كما يجب عليهم أن يحتفظوا بنسخ نظيفة غير مصابة من البرامج لتكون جاهزة في حال حدوث أي عطل. ويجب أن يكون الأشخاص المدربون القادرون على استقبال نظام الكمبيوتر في الخدمة متواجدين على مدار الساعة تجنباً لحدوث مثل هذه المشاكل. ربما يكون أهم عمل يقوم به الشخص المسؤول أو مدير الإدارة هو تسجيل أي بريد إلكتروني مشكوك فيه أو أي نشاط غير طبيعي بالكمبيوتر. ومن الضروري تأمين وحدة مناوبة لمقدمي خدمة الإنترنت وموظفين قانونيين للكشف عن بدء الهجوم الإلكتروني سواء حدث ذلك ضمن مؤسستك أو من عامل خارجي. وتذكر أن هجمات كاليفورنيا قد اكتشفت بواسطة عمال مراقبة محليين فطنين.

هجوم رفض الخدمة DoS

لا يعتبر هجوم رفض الخدمة فيروساً، بل هو طريقة يستخدمها قراصنة الكمبيوتر لمنع أو رفض شرعية وصول المستخدمين إلى الكمبيوترات أو الخوادم. قد يكون فقدان الخدمة ببساطة على شكل عدم قدرة خدمة الشبكة على استخدام البريد الإلكتروني، أو فقدان اتصال الكمبيوتر بالشبكة والخدمات. إن أكثر أنواع "هجوم رفض الخدمة" شيوعاً ببساطة هو إرسال مرور إلى عنوان الشبكة بشكل أكثر من

المبرمجين الذين خططوا مخازن بياناتها المؤقتة المتوقعة. وقد يكون المهاجم على علم أن النظام المستهدف فيه ضعف يمكن استغلاله، أو أنه يحاول الهجوم دون أن يعلم مسبقاً أنه سينجح في ذلك. مثال على ذلك، تخيل أن الإرهابي أنشأ برنامجاً يتصل على الرقم ١-١- ٩ وبدأ عامل التشغيل يجيب على الهاتف وهو يدرك أن هذا الشيء مجرد مزاح. وأخذ البرنامج يعيد هذا العمل باستمرار؛ فإن هذا يمنع العملاء الشرعيين من استعمال هذا البرنامج، لأن الخط سيكون مشغولاً. هذا يسمى رفض الخدمة وهو يجسد "هجوم رفض الخدمة ". يستطيع العديد من أدوات " هجوم رفض الخدمة " نشر هذا الهجوم. مثال ذلك، أن يقوم الإرهابي وبشكل سري بزرع برنامجه في عدة كمبيوترات عبر الإنترنت. وسيحظى هذا العمل بتأثير أكبر لأنه سيكون هنالك اتصال من عدد أكبر من الكمبيوترات مع عمال ١-١-٩ وسيكون من الصعوبة تحديد موقع المهاجم لأن البرنامج لا يشغل من كمبيوتره ويستطيع المهاجم التحكم بالكمبيوتر الذي تم تحميل البرنامج عليه سراً. في أسوأ الأحوال، يمكن لهجوم رفض الخدمة أن يجبر الموقع المتصل بالإنترنت على وقف العملية. ولو كانت تلك العملية التي جرى إيقافها عبارة عن نظام تحكم خطير، فإن المؤسسة ستخسر استعمال وظيفة التحكم تلك. كما يمكن لهجوم رفض الخدمة أن يدمر البرامج والملفات في نظام الكمبيوتر. على كل حال؛ إنه نوع من الخرق الأمني لنظام الكمبيوتر والذي لا يؤدي عادة إلى سرقة المعلومات أو خلل أمني آخر. ورغم أنه عادة ما يكون خبيثاً ومقصوداً، لكن يمكن أن يحصل بالصدفة أحياناً.

كيف يمكن لبرنامج مضاد الفيروسات أن يساعد ضد "هجوم رفض الخدمة"؟

باستخدام الفيروس، يمكن لأدوات " هجوم رفض الخدمة " أن تُحمّل سراً على عدد كبير من أنظمة الكمبيوتر السليمة. تسمى الأنظمة التي لا تعلم أن هذه الأدوات محملة عليها " أنظمة عملاء الجهل " أو طائرات بدون طيار drones أو عملاء

زومبي zombie. ويستطيع القراصنة إدارة أنظمة زومبي مركزياً بهدف شن هجوم رفض الخدمة على كمبيوترات مستهدفة. لا يعتبر عملاء زومبي ضحايا هجوم رفض الخدمة بل جرى استخدامهم من أجل القيام بالهجوم الحقيقي. تقوم برامج المضادة للفيروسات بالكشف عن الفيروسات التي تستطيع إصابة العملاء لكنها لا تكشف " هجوم رفض الخدمة ". كما أن البرامج المضادة الفيروسات يمكن أن تكشف البرامج المؤذية في النظام المصاب وتحديد وقت القرصنة السرية للعملاء. من الصعب تتبع منشأ طلبات " هجوم رفض الخدمة " خاصة لو كانت تلك الهجمات موزعة، كما أنه يستحيل إيقافها، ولكن يمكن لإداريي الخادم أن يقوموا بتدابير احتياطية من شأنها إنقاص خطورة الإصابة بهذا النوع من الهجمات. ولن تكون هذه التدابير الاحتياطية موضع بحثنا في هذا الفصل. على أية حال يمكنك أن تحفظ نظامك من " هجمات رفض الخدمة " وألا تصبح من عملاء زومبي عن طريق تحديث برنامجك المضاد للفيروسات بشكل دائم والالتزام بقواعد ممارسة الحوسبة السليمة التي ذكرناها آنفاً.

الهجمات ضد مزود الطاقة

Attacks Against the Power Supply

هجمات القوة الغاشمة

إن الهجمات ضد مزود الطاقة هي طريقة التخريب التي سبقت الحرب العالمية الثانية. تدرك المؤسسة العسكرية الأمريكية الأهمية القصوى لإمدادات الطاقة للدول الصناعية. وقد شمل قصف الأهداف الإستراتيجية الهامة في الحرب العالمية الثانية مثل السدود (الطاقة الكهرومائية)، محطات المولدات، وأنظمة توزيع الطاقة. أصبحت الولايات المتحدة أكثر اعتماداً على الطاقة الكهربائية في عمليات أنظمة الخدمات الإسعافية، واتصالات هذه الأنظمة والكثير من الخدمات والأجهزة التشخيصية في

المشافي. لو لم تكن أنظمة التحكم والقيادة تمتلك الطاقة الكهربائية، لكانت وببساطة مجرد مجموعة أسلاك، وقطع معدنية وبلاستيكية، ونظام بدون وظيفة. يتوجب على شخص واحد فقط القيام بفحص نتائج الانقطاع المفاجئ لمزود الطاقة من أجل توضيح هذه النقطة بيانياً. رغم أن مزود الطاقة الإسعافية يتوفر في كل الأنظمة الرئيسية مثل المشافي والاتصالات التابعة إلى الخدمات الإسعافية والشرطة والإطفاء والإرسال، وأنظمة المصاعد العالية، فإن مدة هذه الطاقة الإسعافية عادة ما تكون ٢٤ ساعة. وبعد هذه المدة تفقد الطاقة الإسعافية الوقود، وتستنفذ المولدات الاحتياطية والبطاريات أوقات عملها الممكنة. قد يترافق الهجوم على إمدادات الطاقة مع أنواع هجوم أخرى بهدف تحقيق زيادة في التعطيل. وتتراوح الهجمات من حالة بسيطة من قصف فردي محمول ضد محول طاقة رئيسي إلى حالة معقدة من الهجوم الغاشم المتعمد على محطة للطاقة النووية وهذا يخيفنا بسبب احتمال حدوث تسرب إشعاعي والذي تمت تغطيته بالفصل الرابع عشر. في حرب الخليج ١٩٩١م، استخدمت صواريخ كروز مع "القنابل الطرية" بشكل واسع في العراق، وقد قامت هذه القنابل بنشر أسلاك الغرافيت الناقلة والمعادن الأخرى في الهواء الطلق عبر أقنية التحويل التي توصل محطات الطاقة إلى شبكة التوزيع الكهربائي. وعندما وقعت خيوط الغرافيت على الأسلاك الكهربائية في محطات التحويل، تسببت بإضعاف خطوط الطاقة وإرسال إشارات كهربائية إضافية حادة عبر شبكة الطاقة. وقد نشأت فكرة هذا النوع من القنابل من تجربة في جنوب كاليفورنيا، حيث كان الطيران الحربي يرمي بقايا مئات من الشرائح المعدنية بقصد التشويش على رادار العدو. قامت الطائرة بإلقاء حمولتها قرب محطة تحويل الطاقة وسقط الكثير من الشرائح في تلك المحطة، مما تسبب بإضرام العتمة (انقطاع التيار الكهربائي) في مساحات كبيرة من مقاطعة أورانج "كاليفورنيا".[٨] وقد استخدمت هذه القنابل في العراق، كوسوفو، وصربيا. قام العديد من رعاة الإرهاب بتجربة هذه

التقنية التي تهدف إلى تعطيل مزود الطاقة. لا يوجد أدنى شك أن هذا البحث قد تناوله هؤلاء الذين يدرسون الإرهاب، وسوف يكون هدفاً للإرهابيين في المستقبل. إن الأجهزة الارتجالية، مثل شرائط ميلر المغلفة بالألمنيوم والأسلاك المعدنية الورقية يمكن أن تستعمل لإحداث ذلك النوع من التدمير.

الأجهزة الكهرومغناطيسية النبضية

Electromagnetic Pulse Devices

تقوم الأسلحة الكهرومغناطيسية النبضية والتي تعرف أيضاً باسم قنبلة " E " بتوليد نبض من الطاقة قادر على إحداث تقصير الدارة في نطاق واسع من المعدات الإلكترونية بما فيها الكمبيوترات، الأجهزة اللاسلكية، ومزودات الطاقة للمرافق العامة (الشكل رقم ١٥– ١). كان هنريك هيرتز أول من وصف هذه الأسلحة عام ١٨٧٠م، وقد لوحظت تأثيرات هذه الأسلحة ثانية بعد التجارب المبكرة التي تمت على الأسلحة النووية. عندما تفجرت الأسلحة النووية، أنتجت أيضاً حقلاً كهرومغناطيسياً نبضياً محدوداً (يقاس بالنانو ثانية) والذي ينتشر بعيداً عن القنبلة على شكل موجات ويمكن لهذا النبض القصير جداً من الطاقة الكهرومغناطيسية أن ينتج جهداً كهربائياً عابراً يقاس بآلاف الفولتات، وذلك على النواقل الكهربائية المعرضة مثل الأسلاك، الشرائح الإلكترونية، ومسارات التوصيل على ألواح الدارات الكهربائية المطبوعة.

الشكل رقم (١٥–١). الحلقات الخمسة لوراد التي تبين نموذج الهجوم الجوي الإستراتيجي في إطار مجموعات الأهداف المعرضة للهجوم الكهرومغناطيسي. جون واردن هو مؤلف عملية الرعد، وهي خطة القصف الإستراتيجية التي استعملت في حرب الخليج عام ١٩٩١م.

ويمكن لهذه الجهود الكهربائية العابرة أن تدمر أو تؤذي الدارة الإلكترونية في الجهاز. كما يمكن لهذا الجهاز المتضرر أن يستمر بالعمل ولكن قد تكون مصداقيته تأذت بشدة. وقد يعمل بشكل متقطع وهذا ربما يكون مزعجا أكثر من توقفه عن العمل. يكون الجهاز الكهرومغناطيسي النبضي فعالاً فقط في مناطق محدودة حوله. ومن غير الصعب قياس قوة الحقل الكهرومغناطيسي في جهاز معين إذا أعطينا قيمة قطر ذلك الحقل، بينما يكون تقدير احتمال "القتل الإلكتروني" أكثر صعوبة. ويمكن للجهاز

الكهرومغناطيسي النبضي الكبير أن يدمر كل الاتصالات والأجهزة متوسطة النقل التي تقع على مسافة تبعد عنه عدة أميال وفي جميع الاتجاهات.

تعتمد قدرة الجهاز الكهرومغناطيسي النبضي في إبادة المعدات الإلكترونية على الطاقة المولدة وخصائص النبض، فالموجات النبضية القصيرة مثل " الميكروويف " أكثر فعالية ضد المعدات الإلكترونية وبنفس الوقت تكون الحماية منها تكون أكثر صعوبة. كما تعتبر الموجات النبضية القصيرة أكثر خطورة لأنها تنتج طاقة أكبر من طاقة السلاح المفترضة مع طيف ترددي أوسع نطاقاً وهذا ما يؤمن توصيل الطاقة إلى الأجهزة المستهدفة. تعتبر المعدات المزودة بهوائي مصمم على نقل الطاقة من وإلى الجهاز أكثر عرضة للأسلحة الكهرومغناطيسية النبضية وهذا ما يسمى "اقتران الباب الأمامي" front door coupling حيث يمكن للطاقة الصادرة من السلاح الكهرومغناطيسي النبضي أن تدخل الجهاز عبر الهوائي بسهولة وتحدث فيه ضرراً. ويحدث أفضل نقل للطاقة عندما يكون طول الموجات النبضية قريباً من طول موجات الهوائي أو أضعافاً منه. وتكون أجهزة استقبال الردايوهات UHF,VHF والتلفزيونات والهواتف النقالة أكثر عرضة لتأثيرات الأسلحة الكهرومغناطيسية بآلية " اقتران الباب الأمامي ". اليوم، تستعمل معظم أجهزة الاستقبال توليفات ترددية يجري التحكم بها من الكمبيوتر، وقد عبرت العديد من هذه الأجهزة هذه الحقيقة باستخدام كلمات مثل: توليفات، كوارتز، PLL على لوحاتها الأمامية ومنشوراتها. وتوفر هذه التوليفات التي يسيطر عليها الكمبيوتر فوائد هائلة لعمل أجهزة الاستقبال، ليس فقط عن طريق تمكين الأجهزة من الحصول على نفس الثباتية باعتبار الكوارتز هو المرجع الوحيد، بل عن طريق توفير إمكانيات أخرى لهذه الأجهزة وذلك بسبب سهولة التحكم بها عن طريق المعالجات الدقيقة، وتشمل هذه الإمكانيات ذاكرة متعددة، مدخل تردد لوحة المفاتيح، المسح والكثير من الإمكانيات يمكن أن تدرج في اللائحة.

يحصل "اقتران الباب الخلفي" back door coupling عندما يولد الحقل الكهرومغناطيسي الناتج عن السلاح تياراً عابراً كبيراً في أسلاك البنية التحتية التي تتصل بالجهاز. والتي تتضمن أسلاك الهواتف وكابلات الشبكة وخطوط الطاقة. في حالة كمبيوتر السيارة، تكون أسلاك البواجي، أسلاك الوصل بين الحساسات والكمبيوتر، أسلاك الطاقة الواصلة إلى البطارية والمولد الاحتياطي إلى الكمبيوتر وسائل كافية للنبض لكي يدخل كمبيوتر السيارة. يكون كل من يعيش في منطقة معرضة للبرق على معرفة بسيطة بالطاقة الكهرومغناطيسية المترافقة مع ضربة البرق لشبكة الطاقة المحلية والتي يمكنها تدمير الكمبيوترات، التلفزيونات والتليفونات. وتكون النبضات الصادرة من البرق أطول ومخزنة في تيارات ضمن شبكة الطاقة المصممة على كتم الارتفاعات الكهرومغناطيسية. وتكون هذه الزيادة المستمرة في شبكة الطاقة مساوية لاقتران الباب الخلفي. من السهل انتشار السلاح الذي يمتلك مثل هذا التأثير، لأن بعض أسلاك التوصيل ستوجَّه بشكل مناسب لامتصاص بعض الطاقة الكهرومغناطيسية. وستتأذى المعدات الكهربائية، البضائع الإلكترونية المستهلكة، والكمبيوترات، ومعدات الاتصال بشدة بسبب " اقتران الباب الخلفي ". توجد أربعة أنواع أساسية من الأسلحة الكهرومغناطيسية: الأسلحة النووية، المولدات الديناميكية المائية المغناطيسية المحركة بالوقود، مولدات ضغط الدفق والضخ التفجيري، مولدات الموجات الدقيقة عالية الطاقة (بناءً على مؤشر الأشعة المهبطية الافتراضية أو تقنية فيراكتور viractor technology.

الأسلحة النووية Nuclear Weapons

أول ما لوحظ تأثير الأسلحة الكهرومغناطيسية عام ١٩٦٢م وذلك من خلال ترافقه مع الأسلحة النووية، وذلك عندما تم تفجير ١,٤ ميغاطن من المواد النووية على ارتفاع ٤٠٠ كم وسط المحيط الأطلسي. وقد دمر النبض الصادر من الانفجار المعدات

الإذاعية ومعدات الأقمار الصناعية، بينما عطلت التأثيرات الشاردية الاتصالات الإذاعية عالية التردد لمدة ٣٠ دقيقة. وقد أثمر هذا الحادث الكهرومغناطيسي عن فشل نظام الطاقة في أماكن بعيدة مثل هاواي. وقد أسفر التفجير النووي الذي تم على ارتفاع كبيرعن تدفق فوري لأشعة جاما التي نتجت عن التفاعلات النووية داخل السلاح النووي. وتقوم هذه الفوتونات بدورها في إنتاج إلكترونات حرة عالية الطاقة تتناثر على ارتفاعات عالية ٢٠-٤٠ كم تقريباً، لا تلبث أن تحتجز في الحقل المغنطيسي للأرض، مما يؤدي لارتفاع في التيار الكهربائي المتناوب وهذا التيار غير متناظر عموماً ويقوم بإنتاج طاقة كهرومغناطيسية. ويوفر احتجازالإلكترونات الذي يحدث بشكل متزامن بالأساس إشعاعاً منسقاً من مصدر كهرومغناطيسي ضخم جداً. يمكن أن يمتد النبض بسهولة إلى مناطق بحجم القارات، ويمكن لهذا الإشعاع يمكن أن يؤثرعلى الأنظمة على الأرض، البحر، والهواء. يمكن أن يؤثر التفجير النووي كبير على ارتفاع ٤٠٠ – ٥٠٠ كم فوق كانساس على جميع الولايات المتحدة، ويمكن للإشارة الصادرة من هذا الحادث أن تمتد إلى الأفق المرئي وكأنها تشاهد من موقع نقطة الانفجار. على المستويات الأقل، يكون تأثير الانفجار النووي على الكهربائيات مختلفاً، ينتج "النبض الكهرومغناطيسي الناشئ في منطقة المصدر" (SREMP) من الانفجار النووي على ارتفاع منخفض. يتشكل التيار الإلكتروني العمودي بسبب توضع غير متناظر للإلكترونات في الفضاء والأرض والذي ينجم عن الانفجار النووي، إن تشكيل واضمحلال هذا التيار يصدر نبضاً إشعاعياً كهرومغناطيسياً. إن الانفجار على المستويات المنخفضة ينتج نبضاً غير متناظر، لأن بعض الإلكترونات المرسلة نحو الأسفل تحتجز على سطح الأرض، بينما تتحرك الإلكترونات الأخرى نحو الأعلى والخارج لمسافات بعيدة في الفضاء، مما ينتج تشرد وانفصال شحنات. يمكن أن تتواجد مستويات من الحقل الكهربائي أكبر من ١٠٥ V/m ومستويات من الحقل

المغناطيسي أكبر من ٤٠٠٠ A/m في منطقة المصدر، وتكون سعة هذا النبض أكبر بكثير من مثيلاتها الناجمة عن الانفجارات النووية التي تحصل على الارتفاعات العالية أو ضربات البرق، وهي تمثل تهديداً كبيراً لكل أنظمة كمبيوترات المدنيين وأغلب المعدات الإلكترونية في المنطقة المتضررة. تشكل الأرض طريق العودة للإلكترونات على الجزء الخارجي لمنطقة الترسيب باتجاه نقطة الانفجار. إن الشوارد الموجبة، التي تسافر لمسافات أقصر من الإلكترونات وعلى سرعات أقل، تبقى في الخلف وتتحد مع الإلكترونات التي عادت من الأرض. ولهذا فإن الحقول المغناطيسية القوية تنشأ أيضاً في منطقة " نقطة الصفر " على الأرض. عندما يحدث الانفجار النووي قرب الأرض، فإن بؤرة النبض الكهرومغناطيسي الناشئة في منطقة المصدر قد لا تقع في الحقل الكهرومغناطيسي البعيد، بل ربما تقع في منطقة التحريض الكهرومغناطيسية. وبالنتيجة، تبعد المنطقة الأكثر تضرراً ٣-٨ كم من نقطة الصفر على الأرض، حيث تتأذى المعدات الكهربائية المنزلية في هذه المنطقة بشدة بسبب الانفجار والصدمة.

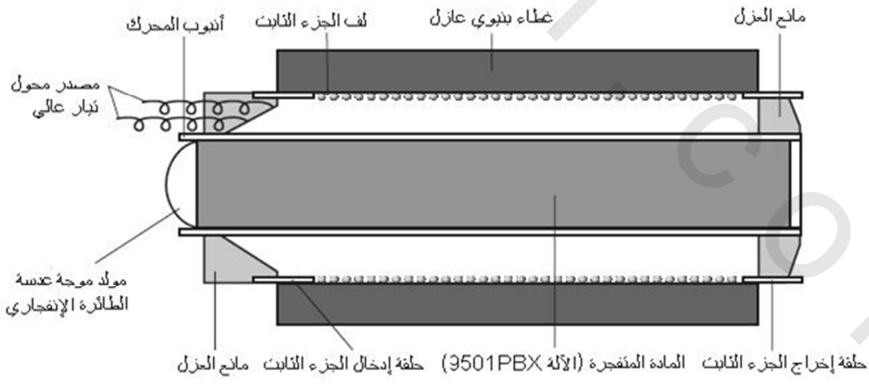
المولدات الهيدروديناميكية المائية المغناطيسية Magnetohydrodynamic Generators

لم تناقش تقنية الانفجار والدفع التي تعتمد على المولدات الديناميكية المائية المغناطيسية بشكل جيد في تقارير المصادر المفتوحة، بينما تم بحث تقنية المولدات الديناميكية المائية المغناطيسية بشكل واسع في الاتحاد السوفيتي السابق علماً أنها لم تستخدم بعد في أنظمة الأسلحة. وتكمن الميزة الكبرى لهذه المولدات في قلة أجزائها المتحركة وصغر أحجامها، وقد تركزت معظم الجهود الروسية في البحث على إمكانية أن تكون هذه المولدات مصدراً للطاقة الكهربائية المكثفة أكثر من أن تكون نظام سلاح.

مولدات ضغط الدفق Flux Compression Generators

قد تكون أجهزة الانفجار القديمة أفضل مصدر للطاقة وذلك من خلال توليد نبض غير متكرر قوي وخطير. يمكن أن تتحول الطاقة المخزنة في ١ كيلوطن أو ٢

كيلوطن من مادة TNT إلى نبض كبيرمن الموجات الدقيقة وذلك باستخدام جهاز يسمى " ضاغط الدفق ". يستخدم هذا الجهاز طاقة الانفجار من أجل ضغط التيار وحقله المغناطيسي في حجم أصغر، يولد إرسال هذا النبض عبر الهوائي انفجاراً مميتاً في الموجات اللاسلكية والموجات الدقيقة. تعتبر بساطة مولدات ضغط الدفق ذات أهمية كبيرة في جذب الإستراتيجيات العسكرية والإرهابية على حد سواء، حيث إن أجهزة مولدات ضغط الدفق هي أجهزة محمولة ويمكن تشغيلها عن بعد. يتألف الجهاز من أنبوب نحاس أسطواني مليء بمواد متفجرة عالية الطاقة وسريعة الانفجار، ويحيط بهذا الأنبوب لفائف حلزونية من أسلاك نحاسية ثقيلة لها قرن هوائي يكون متصلاً بالنهاية البعيدة (الشكل رقم ١٥-٢). يقوم المكثف بالتفريغ في هذه اللفائف لينتج حقلاً مغناطيسياً قبل انفجار المواد المتفجرة. يؤدي وضع إعدادات المفجر بحالة إيقاف إلى تحريض المادة المتفجرة وإرسال مقذوف الانفجارعلى طول الأنبوب بسرعة ٥٤٠٠ مل/ثا تقريباً.



الشكل رقم (١٥-٢). تفاصيل البنية النظرية لمولدات ضغط الدفق والأجهزة الكهرومغناطيسية النبضية.

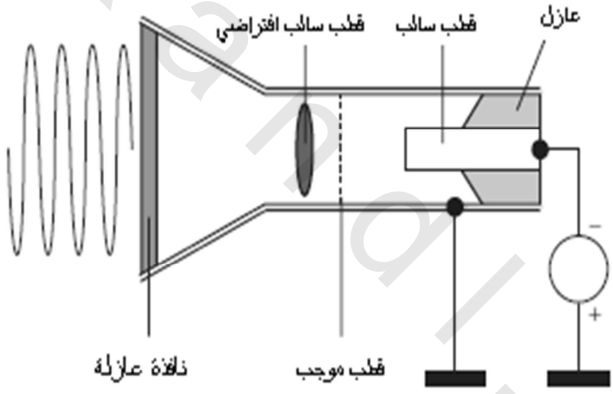
ومع تقدم الانفجار، تكوّن "اللفائف" الغطاء الهيكلي للمادة غير المغناطيسية. قبل أن تبدأ موجة الضغط الانفجاري بهدف تحطيم الجهاز، تصدر نيران الانفجار من الأنبوب المعدني الداخلي. يسبب بقاء المعدن المشوه على اتصال باللفائف دارة قصيرة تقوم بتحويل التيار والحقل المغناطيسي الذي أنتجته إلى اللفائف السليمة الموجودة في الخلف. ومع تقدم الانفجار ضمن الأنبوب المعدني ينضغط الحقل المغناطيسي في حجم أصغر فأصغر. ومع انضغاط الحقل المغناطيسي هذا يحصل ارتفاع ضخم في تيار اللفائف قبل حدوث الانفجار، مما يولد نبضاً بمقدار١ميغا- أمبير لمدة ٥٠٠ بيكو ثانية تقريباً. أخيراً، وقبل تحطم كامل السلاح في الانفجار، يمر نبض التيار في الهوائي، الذي يقوم بإشعاع الطاقة الكهرومغناطيسية للخارج. وكل هذا يحصل في مدة تقل عن عُشرميلي- ثانية، وخلال هذا العشر من الميلي- ثانية، تتولد وتنتشر طاقة بمقدار١ تيرا- واط. يمكن أن يستخدم مولد ضغط الدفق الصغير من أجل بدء التيار في جهاز أكبر. في هذه الحالة، يمر نبض التيار في لفائف أكبر قبل أن تنفجر المواد المتفجرة في الجهاز الكبير، بشكل يكرر العملية السابقة على نطاق أوسع. وفي ذروة العملية، قد يقوم جهاز ضغط الدفق الكبير بإنتاج عشرات التيرا- واطات من الطاقة، بما يعادل أكثر من ألف من ضربات البرق. وتقوم الأسلحة التي تستخدم هذه التقنية بإنتاج معظم طاقتها في ترددات أقل من ١ ميغا هيرتز مما يجعل التركيزعلى الطاقة أمراً صعباً. إن تفجير الأسلحة الكهرومغناطيسية في الهواء قرب الطوابق العلوية لناطحات السحاب يزيد من تأثيراتها. هذه الأسلحة رخيصة وبسيطة. يعتبر إنتاج الإلكترونيات والمواد المتفجرة المستعملة في صناعتها، والتي لا تتوفر عادة في المتاجر المحلية للإلكترونيات، أسهل بكثير من إنتاج أيٍّ من المواد النووية. إن أية دولة أو مجموعة إرهابية كبيرة تمتلك الرسوم الهندسية وخصائص هذه الأسلحة يمكنها بسهولة إنتاجها وبأسعار زهيدة لا تتجاوز ٢٠٠٠ دولار للواحدة.[٩] وباعتبار روسيا والصين، اللاعبين

الرئيسين في هذا المجال، تعانيان من صعوبات اقتصادية، يبقى انتشار هذه الأجهزة أمراً وارداً جداً.

مولدات الموجات الدقيقة عالية الطاقة

لا تزال مصادر مولدات الموجات الدقيقة عالية الطاقة تخضع للدراسة منذ سنوات عديدة باعتبارها أسلحة يمكن استعمالها في حالات متنوعة مثل القتال والتخريب وتطبيقات إرهابية. وبسبب القيود المفروضة على تصنيفها، تبقى تفاصيل هذا العمل غير معروفة نسبياً خارج مجتمع المؤسسة العسكرية ومقاوليها، تسمى هذه الأسلحة أحياناً أسلحة ترددات لاسلكية عالية الطاقة. يعتبر الفيراكتور أكثر سلاح في مولدات الموجات الدقيقة عالية الطاقة بساطة وهو (مؤشر أشعة كاتود الافتراضي) الذي يتصل بمكثف كبير لتأمين تيار عالٍ خلاله. هنالك أجهزة أخرى يمكن استعمالها لإنتاج مولدات الموجات الدقيقة عالية الطاقة وهي تشمل المغنطرون (جهاز يوجد في كل فرن ميكروويف)، كليسترون، والصمام الثلاثي المنعكس. يقوم الفيراكتور الأساسي بإنتاج مجال إلكتروني قوي جداً موجه ضد شبكة القطب الموجب (الصواعد) خلال الأنبوب. حيث تمر كثير من الإلكترونات عبر القطب الموجب وتشكل فقاعة من شحنة فراغية – كاتود افتراضي – خلف القطب الموجب. لو وضع هذا الكاتود الافتراضي في تجويف صدوي محكم، فإنه يمكن توليد موجات دقيقة عالية الطاقة. الفيراكتور جهاز صغير الحجم، بسيط ميكانيكياً، متين وقادر على إنتاج نبض إشعاعي قوي جداً يتراوح من ٧٠ كيلو واط وقد يتجاوز ٤٠ جيجا واط في ترددات الموجات الدقيقة. وتتحدد مدة النبض الناتج حسب درجة ذوبان القطب الموجب. (الشكل رقم ١٥-٣). يمتلك الفيراكتور أهمية خاصة، كونه يركز على الطاقة الناتجة وإمكانية استخدام جهازين منه ضمن المعدات وذلك من خلال فتحات التهوية، والفراغات البينية في الدرع الضعيف المغطي الواقي. النقطة المهمة الواجب تذكرها هي الطبيعة

الغدارة لمولدات الموجات الدقيقة عالية الطاقة. وبسبب حزمة ترددا تها التي تتراوح بين ٤–٢٠ جيجا هيرتز، تستطيع هذه الأسلحة المرور عبر الهوائي، وأيضاً من خلال فتحات الدرع في المعدات. تشير العديد من التقارير إلى أن النسخة المحمولة الصغيرة من الجهاز يمكن أن تستخدمها قوات الشرطة بهدف توقيف السيارات وذلك عن طريق قدرة هذه الأجهزة على إغلاق الكمبيوترات التي تتحكم بالمحرك.[١٠] وتفيد تقارير أخرى بأن المجرمين يستخدمون هذه الأجهزة لتدمير الأجهزة الإلكترونية الأمنية في البنوك والمستودعات، قبل سرقتها.



الشكل رقم (١٥–٣). الفيراكتور.

الآثار المترتبة

تشكل أسلحة مولدات الموجات الدقيقة عالية الطاقة والأسلحة الكهرومغناطيسية تهديداً هاماً للمعدات الإلكترونية المعرضة للأذية بسبب موجات الطاقة العابرة. تعتبر الأسلحة الكهرومغناطيسية أسلحة دمار شامل جرى ضبطها بشكل خاص حسب نقاط الضعف الموجودة في المدن الحديثة التي تعتمد على الكمبيوتر.

تستطيع أسلحة مولدات الموجات الدقيقة عالية الطاقة والأسلحة الكهرومغناطيسية التقليدية تعطيل الأجهزة الإلكترونية غير المغطاة بدرع حماية وذلك ضمن نطاق تأثيرها. (صممت أغلب المعدات الإلكترونية والأجهزة اللاسلكية العسكرية من أجل مقاومة بعض مستويات الأسلحة الكهرومغناطيسية، لكن المعدات المدنية ليست مدرعة بالشكل الكافي لمثل هذا النوع من الهجوم). تبقى دارات معدات الكمبيوتر التجارية معرضة للأسلحة الكهرومغناطيسية (حتى الدارات المتواجدة في أنظمة تشغيل في السيارات والشاحنات وإشارات المرور). تتألف هذه الدارات عادة من أجهزة معدنية مؤكسدة عالية الكثافة نصف ناقلة حساسة إلى التعرض للفولتاج العالي العابر. ويتطلب تدمير هذه الأجهزة كلياً طاقة قليلة جداً. إن الكمبيوترات التي تستخدم أنظمة معالجة البيانات، أنظمة الاتصالات والعرض، تطبيقات المراقبة الصناعية، بما فيها إشارات الطرق والسكك الحديدية والتطبيقات المدمجة في المركبات، أجهزة المراقبة القلبية، أجهزة التحكم بالمحركات الرقمية والطيران الإلكتروني ومعالجات الإشارة (تتواجد في أنواع عديدة من المعدات اللاسلكية الحديثة)، تكون عرضة لتأثيرات الأسلحة الكهرومغناطيسية من خلال " اقتران الباب الخلفي ". وتكون شبكات الكمبيوتر على وجه الخصوص عرضة لهذه الإصابة، لأن مئات الأقدام من الكابلات الموصلة إلى محطات العمل يمكن أن تقوم بوظيفة الهوائي المستقبل للموجات اللاسلكية الفعَّالة. يعتبر الكمبيوتر وحدة التحكم الإلكتروني في السيارات الحديثة وأغلب المركبات. وتضم التوصيات الصادرة من وكالة حماية البيئة عام ١٩٧٠م والتي تهدف إلى إنقاص الانبعاثات، التوجه القوي من أجل الانتقال إلى المحركات ذات التحكم الإلكتروني وإدخال الكمبيوتر إلى كل المركبات وتتواجد هذه الكمبيوترات في كل سيارات الإطفاء والإسعاف سواء كانت معتمدة على الديزل أو الغازولين. يقوم نظام الكمبيوتر بالإيعاز إلى المحرك عن قدوم الوقت الضروري لتوفير الوقود والهواء لأسطوانات المحرك. كما أنها

ترسل وتستقبل الإشارات من حساسات المحرك وإليها من أجل الوصول إلى أفضل وضعية اقتصادية للوقود. بدأت قوانين الفيدرالية الأمريكية فيما يخص التحكم بمحركات المركبات عن طريق الكمبيوتر بالتأكيد على ضرورة تطبيق حساسات الأكسجين عام ١٩٨٢م. وكان أولها القانون الفيدرالي الأمريكي الأول رقم IM-240. ومنذ ذلك الحين بدأ العمل على تطوير النظام الأساسي (نظام التشخيص الكمبيوتري على متن المركبة OBD) إلى النظام الفيدرالي الأمريكي الحالي عام ٢٠٠٣م OBD-II (والذي طبق على مركبات الولايات المتحدة بالإضافة إلى المركبات الموجودة حول العالم بعد مصادقة الاتحاد الأوروبي). وباعتبار أن الأسلحة الكهرومغناطيسية تستطيع تعطيل هذه الكمبيوترات الضرورية والموجودة على متن المركبات فإن هذه المركبات لن تتمكن من الاستمرار بالعمل. وبسبب الاعتماد العالمي في الولايات المتحدة على الإلكترونيات، فإن الأسلحة الكهرومغناطيسية بإمكانها أن تحدث شللاً في نظام الخدمات الطبية الإسعافية والذي يعتمد على الكمبيوترات وشبكات الكمبيوتر وأنظمة الاتصالات الإلكترونية. يمكن أن يمتد هذه الضرر الناجم عن الإرهاق الزائد للدارات الإلكترونية إلى مسافة بعيدة عن المنطقة التي تأثرت بشكل مباشر بانفجار وإشعاع السلاح النووي. في مثل هذا الهجوم، قد نفقد الطائرات المدنية. باختصار، سيفقد الطيارون الاتصال والمساعدات الملاحية، وأنوار الهبوط، وفي بعض الأحيان يحصل فقدان القدرة على التحكم بالطائرة بعد تدمير أسلاك الدارات الإلكترونية بواسطة الأسلحة الكهرومغناطيسية الضخمة. قد تقوم أجهزة قياس الطائرة بعرض قراءات صحيحة وهذا العرض قد يومض في أوقات الخطورة. من غير المعلوم ما إذا كان نظام التحكم بالطيران الجوي الدولي أصبح أكثر صرامة وتشدداً ضد الأسلحة الكهرومغناطيسية.[١١] تم وضع تصنيف ملائم لمدى الخطورة التي تشكلها الأسلحة الكهرومغناطيسية على الأنظمة الإدارية الفيدرالية للطيران. رغم أن التصميم الأولي للسلاح يعتبر صعباً من الناحية التقنية، يمكن أن يستفيد الذين

يمتلكون المهارات التقنية والهندسية الأساسية فقط من تقنية الأسلحة الكهرومغناطيسية. يمكن صناعة لأسلحة الكهرومغناطيسية باستخدام مواد متوفرة للحكومات والإرهابيين على حد سواء. كما يمكن أن تتوفر في الأسواق السرية وبأي وقت أسلحة متطورة وجاهزة للاستخدام. وتشير التقارير إلى أن دولة واحدة على الأقل، الهند، قامت بصناعة سلاح كهذا لأغراض سلمية. بالفعل، قامت الولايات المتحدة بنشر مثل هذه الأسلحة، وهذا ما جعل تصميم هذه الأسلحة متاحاً للدول الإرهابية في يومنا هذا.(نشرت الولايات المتحدة الأمريكية أسلحة كهرومغناطيسية في عملية عاصفة الصحراء والتي صممت لتقليد وميض الكهرباء الصادر من القنبلة النووية). يمكن أن توفر لنا التطورات المستقبلية أسلحة من هذا النوع وبأحجام صغيرة، الشيء الذي نحتاجه لنتمكن من تحميلها على رؤوس الصواريخ الحربية أو القنابل. حالياً، لا يصل المدى المجدي للسلاح إلى حجم تأثيرات الأسلحة الكهرومغناطيسية النووية. وكما تدل تقارير المصادر المفتوحة أنه يمكن أن يصل المدى المجدي للسلاح إلى " مئات الأمتار أو أكثر من ذلك ".

الآثار المترتبة والتدابير الوقائية
Implications and Protective Measures

من الصعب توفير الحماية من الأسلحة الكهرومغناطيسية بدون الحصول على معدات اتصال على درجة عسكرية. وعليك أن تلاحظ أن الأسلحة الكهرومغناطيسية يمكن أن تكون متسترة. ويعتبر تدمير الجناة كل الأجهزة الإلكترونية الواقعة ضمن المجال أمراً غير ضروري. وبدلاً عن ذلك، يمكنهم توجيه ضربة قاسية تكون كافية لتحطيم الأجهزة الإلكترونية. ويسمي الجيش هذا الشيء " القتل الناعم " حيث تحدث الأذية حتى بدون علم الضحية. وبحسب تقرير بوب غاردنر، وهو الذي ترأس اللجنة المسؤولة عن الضجة التي أحدثتها الأسلحة الكهرومغناطيسية في الاتحاد الدولي للعلوم

في غنت- بلجيكا.[١٢] استخدم المجرمون أسلحة الموجات الدقيقة. وتفيد التقارير التي أتت من روسيا أن هذه الأجهزة استخدمت لتعطيل الأنظمة الأمنية البنكية وقطع اتصالات الشرطة. وهنك تقرير آخر يفيد بأن بنوك لندن قد تعرضت لهجوم بنفس الطريقة. ومع أن هذه الحوادث يصعب إثباتها، لكنها تبقى معقولة جداً. قال غاردنر، إذا كنت تسأل فيما إذا كان أحد يمكنه من الناحية التقنية أن يقوم بمثل ذلك عندها يكون الجواب نعم.[١٣] هنا نعرض بعض التدابير المضادة للأسلحة الكهرومغناطيسية والتي يمكن أن يتبعها مقدمو الخدمات الطبية الإسعافية:

١- يتم إنجاز طريقة الحماية الوحيدة والموثوق بها ضد انبعاثات الأسلحة الكهرومغناطيسية بواسطة تغليف المعدات المعرضة بدرع معدني من العيار الثقيل أو إحاطته بماسح معدني خاص يسمى قفص فارادي Faraday cage (الشكل رقم ١٥- ٤). يمكن صنع قفص فارادي من شبكة معدنية ناعمة، ويتصل هذا القفص إلى الأرض ويحيط بشكل تام بالعناصر التي يقوم بحمايتها. وقد يسوء وضع الحماية هذا لو قامت كابلات الطاقة، كابلات البيانات، والهوائيات باختراق القفص. قم بحفظ كل المعدات في القفص مفصولاً عن البطاريات أو أي مزود آخر للطاقة.

٢- الحفاظ على إمدادات قطع غيار أجهزة اللاسلكي، المراقبة، وقطع غيار تشغيل المحرك. وقم بحفظ قطع الغيار في قفص فارادي. يمكن أن تحفظ قطع المعدات الأصغر في حاويات ذخائرعسكرية معدنية فارغة أو علب معدنية محكمة الإغلاق بشدة.

٣- استخدم نظاماً واحداً في نفس الوقت خلال فترة التهديد. قم بفصل الأنظمة الأخرى من الطاقة والهوائيات وقم بحفظها في قفص فارادي.

٤- لو فشلت في تشغيل مركبتك، قم بفصل الخط السلبي للبطارية، وانتظر دقيقتين، ثم أعد وصله ثانية وحاول تشغيل مركبتك، لأن بعض أنظمة التشغيل المحوسبة في السيارات الحديثة يمكنها أن تعيد تشغيل المركبة بهذه الطريقة. قد تتمكن

المعدات التي دعمت ضد النواتج الكهرومغناطيسية من الصمود أمام الحقول الكهرومغناطيسية الأكبر. بينما لن تتأثر اللاسلكيات والمعدات الأخرى والتي تستخدم تقنية الأنبوب المفرغ، كون هذه الدارات لا تتأثر بالأسلحة الكهرومغناطيسية. لا يوجد أدنى شك أنه من الواجب تقوية النظام لتجنب أي ضرر يمكن أن يلحق بأي جزء من المعدات الكهرومغناطيسية ؛ على كل حال، تبقى للتقوية هذه محدوديتها. ويمكن تقوية المعدات الجديدة عن طريق تطوير التصميم الخاص بها، بينما يستحيل ذلك في المعدات القديمة. ولأن تطوير ونشر الأسلحة الكهرومغناطيسية يحصل في مرحلة مبكرة، فإنه لا أحد يعرف بالواقع ماذا سيكون تأثيرها الإجمالي. فقط ومن خلال بيانات التي جمعت بأثر رجعي أو ما تم نشره من بيانات عسكرية جمعت خلال تطوير الأسلحة نستطيع أن نخطط بفعالية من أجل الاستعداد لهذه الأسلحة.

الشكل رقم (١٥– ٤). قفص فارادي مع كمبيوتر بداخله. خلال العملية، يغلق الباب. قفص فارادي غير فعال عندما يكون الباب مفتوحاً.

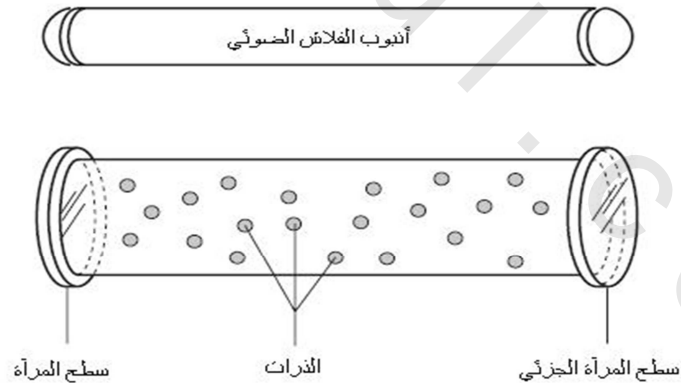
أسلحة الطاقة الموجهة

Directed Energy Weapons

تشمل أسلحة الطاقة الموجهة بواعث الإشعاع بالموجات الدقيقة (الميكروويف)، مولدات إشعاع الجزيئات. وتعتمد أسلحة الطاقة الموجهة على الأمواج الكهرومغناطيسية أو الجزيئات تحت الذرية التي تصطدم في أو قرب سرعة الضوء. لقد جربت العديد من هذه الأسلحة في القتال وقد تكون متاحة للإرهابيين في المستقبل القريب جداً.

خلفية الليزر

هناك تقنيات كثيرة لإنتاج الليزر، وتشمل استخدام الغاز، الكريستال، الصمامات الثنائية متوسطة النقل. وكل هذه التقنيات لها أسس بناء متشابهة. ويمكنك أن ترى كل مكونات بناء الليزر في (الشكل رقم ١٥– ٥) والتي توضح كيف يعمل الليزر القاني ruby laser البسيط.

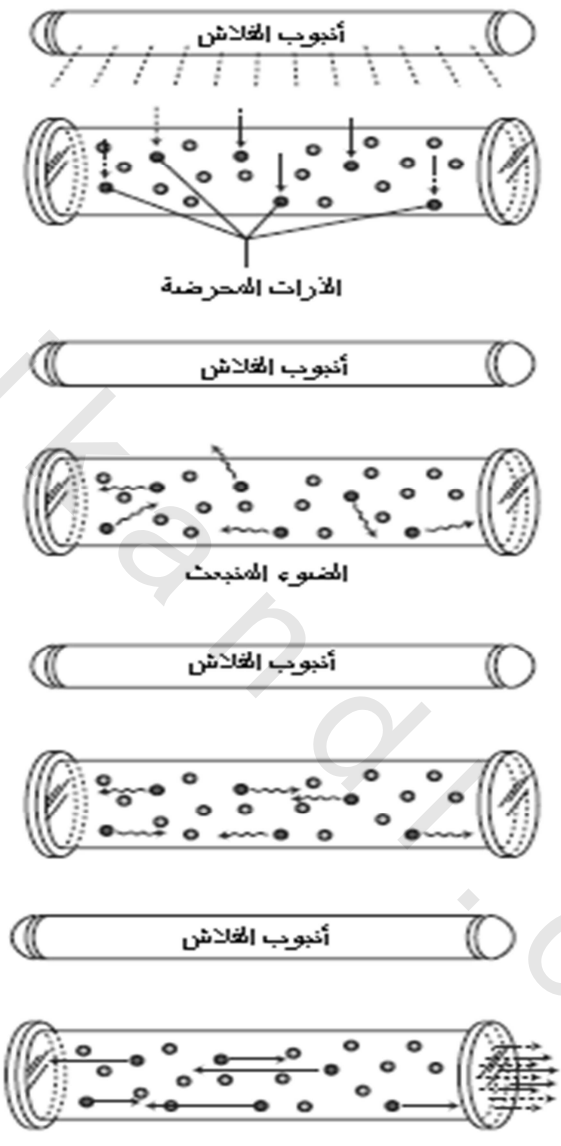


الشكل رقم (١٥– ٥). الليزر القاني ويتألف من أنبوب فلاش، قضيب ياقوتي ومرآتين.

obeikandl.com

أجهزة الليزر Lasers

في عام ١٩٥٤م، ابتكر تشارلز تاونز وآرثرتشاولو " المازر "maser وهو مضخم للموجات الدقيقة بواسطة انبعاث شعاعي محرض). حيث قاما باختراع المازر باستخدام الأمونيا وإشعاع الموجات الدقيقة قبل وضع نظرية الليزر وهو (مضخم للضوء وذلك بواسطة إشعاع منبعث محرض) في عام ١٩٥٨م. إن تكنولوجيا المازر تشبه إلى حد بعيد مثيلتها في الليزر، لكنها لا تستخدم الضوء المرئي. وكان جوردون غولد أول من استخدم كلمة " الليزر" عام ١٩٥٧م. هنالك سبب جيد يجعلنا نصدق أن جوردون غولد هو من قام بصنع أول ضوء ليزري. (قام باستخدام أرقام براءة الاختراع رقم ٤٠٥٣٨٤٥ أو ٤٧٠٤٥٨٣ في مضخمات الليزر ذات الضخ الضوئي ؛ وتستخدم هذه المضخمات الضوئية التصادمات لإنتاج انعكاس ليزري شائع). وبمتابعة أعماله في مشروع مانهاتن، كان غولد طالب دكتوراه في جامعة كولومبيا تحت إشراف تشارلز تاونز، مخترع المازر. وكان جوردون غولد أول من استوحى فكرة بناء الليزر البصري عام ١٩٦٠م خلال عمله رئيساً لقسم مختبرات البحث في هيوز. وابتكر تيودور ميمان الليزر القاني (الياقوت الأحمر) الذي يعتبره البعض أول ليزر بصري ناجح. يتألف الليزر من أنبوب فلاش (كالذي يتواجد بالكاميرات)، وقضيب ياقوتي، ومرآتين (نصف فضي). يشكل القضيب الياقوتي الوسط الليزري، بينما يقوم أنبوب الفلاش بضخ الليزر. ويتم تشكل الضوء الليزري في حالة الليزر القاني من خلال النقاط التالية (الشكل رقم ١٥-٦): يظهر A يقوم أنبوب الفلاش بحرق ودفع الضوء ضمن القضيب الياقوتي ليقوم الضوء بتحريض الذرات في القضيب الياقوتي B بعض هذه الذرات تطلق فوتونات C تنطلق بعض الفوتونات باتجاه موازٍ لمحور القضيب الياقوتي، وترتد ذهاباً وإياباً بين المرآتين D يمر الضوء خلال المرآة نصف فضية مشكلاً الليزر:



الشكل رقم (١٥-٦). A يقوم أنبوب الفلاش بحرق ودفع الضوء ضمن القضيب الياقوتي ليقوم الضوء بتحريض الذرات في القضيب الياقوتي B بعض هذه الذرات تطلق فوتونات C تنطلق بعض الفوتونات باتجاه موازٍ لمحور القضيب الياقوتي، وترتد ذهاباً وإياباً بين المرآتين D يمر الضوء خلال المرآة نصف فضية مشكلاً الليزر.

obeikandl.com

١- يقوم أنبوب الفلاش (المضخة) بحرق ودفع الضوء ضمن القضيب الياقوتي ليقوم الضوء بتحريض الذرات في القضيب الياقوتي.

٢- تطلق بعض هذه الذرات فوتونات.

٣- تنطلق بعض الفوتونات باتجاه موازٍ لمحور القضيب الياقوتي، وترتد ذهاباً وإياباً بين المرآتين، مما يحرض على إطلاق الفوتونات من ذرات أخرى.

٤- ومع انبعاث فوتونات كافية، يمر الضوء خلال المرآة نصف فضية. مما يكوِّن ضوءاً ليزرياً ذا مسارات متوازية، أحادي الطور وأحادي اللون. ويملك هذا الضوء الليزري خصائص خاصة (الشكل رقم ١٥-٧ يظهر A الطبيعة غير المنتظمة للضوء العادي. من المصباح الكهربائي B الطبيعة المنسقة لضوء الليزر).

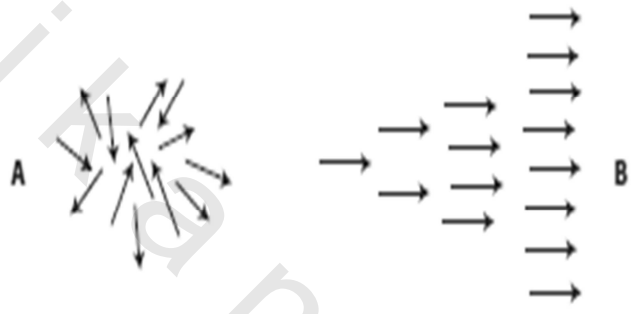
- يكون الضوء المتحرر أحادي الطور، وهذا يعني أنه يحوي طول خاص ووحيد من موجة الضوء أو لون خاص وحيد. إن كمية الطاقة التي تتحرر مع سقوط الإلكترون إلى المدار السفلي هي التي تحدد طول موجة الضوء. كما يعتمد طول موجة الضوء أيضاً على مادة الليزر وطريقة التحريض المتبعة لانبعاث الضوء.

- يكون الضوء المتحرر متماسكاً، بمعنى أنه منظم، فكل خطوة يتحركها الفوتون تكون متزامنة مع الفوتونات الأخرى. (تكون موجات الإشعاع الكهرومغناطيسي في طور الفراغ والزمن) وهذا يعني أن كل الفوتونات تشكل جبهات من موجات يتم إطلاقها بشكل منسجم.

- يكون الضوء موجهاً جداً، وللضوء الليزري شعاع ضيق جداً وقوي جداً ومركز ومن جهة أخرى، يقوم المصباح الكهربائي بتحرير الضوء في جهات عدة، ويكون الضوء ضعيفاً ومنتشراً.

- إن تصميم جهاز الليزر يجعل الشعاع متوازياً.

- أخيراً، وبسبب هذه الطبيعة المتوازية فإن الضوء الليزري لا ينتشرعلى مسافات بعيدة. طور الصليب الأحمر الدولي في عام ١٩٩٠م تصنيفاً مفيداً لليزر بهدف استخدمه في أرض المعركة أو لأغراض اقتصادية. تحدد المواد التي يصنع منها الليزر التردد، وإلى حد ما تحدد الطاقة المتاحة.



الشكل رقم (١٥-٧). A الطبيعة غير المنتظمة للضوء العادي. من المصباح الكهربائي B الطبيعة المنسقة لضوء الليزر.

تصنف كل أنواع الليزر حسب الصنع توضع على شكل ملصقات تحذيرية مناسبة. وتستخدم هذه المعايير في تصنيف الليزر:

١- **طول الموجة:** وهذا يؤخذ بعين الاعتبار في كل أنواع الليزر. لو صمم الليزر من أجل إصدار أطوال موجات متعددة، فإن التصنيف يعتمد على طول الموجة الأكثر خطراً.

٢- **متوسط الطاقة المنتجة وتحدد زمن التعرض:** المرتبطان بتصميم الليزر أيضاً يؤخذان بعين الاعتبار بحالة الليزر مستمر الموجة والليزر ذي النبض المتكرر.

٣- **الطاقة الكاملة بكل نبض** (بالجول)، مدة النبض، تواتر تكرر النبض، والتعرض الإشعاعي الحزمي الناشيء تؤخذ بعين الاعتبار في حالة الليزر النبضي. يبين الجدول رقم (١٥-١) و(١٥-٢) تصنيفين مختلفين لليزر ويبين الجدول رقم (١٥-٣) أنواع الليزر. وبعد تطوير أول ليزر وظيفي، ظهرت فوراً الإمكانية العسكرية (ومن ثم الإرهابية) لليزر، حيث يمكن أن تتجاوز مستويات الطاقة في الليزر النبضي الحديث ملايين الواطات في جزء من الثانية (الشكل رقم ١٥-٨).

الجدول رقم (١٥-١). تصنيف الليزر.

الفئة ١	وهي أجهزة ليزر غير خطرة للنظر المستمر أو أنها صممت بطريقة تمنع وصول الإشعاع الليزري إلى الإنسان. وتتألف من أجهزة ليزر ذات طاقة منخفضة (حتى ٠,٤ ميكروواط) أو ربما أجهزة ليزر تتضمن طاقة أعلى. وقد يكون هنالك أجهزة ليزر ذات خطورة أكثر في سياق هذه الفئة الأولى، لكن بدون تسرب إشعاع مؤذٍ (مثل ليزر الطابعة).
الفئة ٢ أجهزة الليزر المرئية ٤٠٠-٧٠٠ نانومتر	وهي أجهزة ليزر تصدر ضوءاً مرئياً والذي بسبب استجابات النفور البشرية الطبيعية، لا يسبب خطراً بالحالة الطبيعية إلا بالنظر المباشر إليه لمدة طويلة (مثل مصادر الضوء العادية). تندرج المؤشرات الليزرية ضمن هذه الفئة.
الفئة ٢ أ أجهزة الليزر المرئية ٤٠٠-٧٠٠ نانومتر	وهي أجهزة ليزر تصدر ضوءاً مرئياً لا يهدف للمساعدة على الرؤية، وبالحالات العملية العادية لا يتسبب بأي أذية للعين لو تم النظر المباشر إليه لمدة أقل من ١٠٠٠ ثانية (مثال، الماسحات الضوئية ذات شريط الرموز).
الفئة ٣ أ	وهي أجهزة ليزر لا تسبب بالحالة الطبيعية أذية للعين لو نظر إليها للحظات، لكن تشكل خطراً لو تم النظر إليها باستعمال أدوات بصرية تجميعية (المنظار أو العدسة الليفية البصرية). تندرج ضمن هذه الفئة الكثيرمن أجهزة الليزر العسكرية الهدفية. وتعتبر هذه الفئة من الليزر والتي تمتلك طاقة تتراوح بين ١-٥ ميغاواط "خطراً عينياً ثانوياً".

openkandil.com

تابع الجدول رقم (١٥-١).

الفئة ٣ب	وهي أجهزة ليزر تحمل خطورة على العين والجلد إذا تم النظر إليها بشكل مباشر، وهذا يشمل النظر داخل الشعاع أو إلى انعكاسات المرآيا. هذه الأجهزة لا تنتج انعكاساً منتشراً خطراً إلا بالنظر إليها عن قرب. تتراوح طاقة هذه الأجهزة من ٥-٥٠٠ ميغاواط. وتعتبر " خطراً عينياً هاماً ".
الفئة ٤	وهي الأجهزة التي تحمل خطورة على العين من خلال النظر المباشر ومن خلال المنظار والانعكاسات المنتشرة.وهي خطرة على العين والجلد. قد يحمل مثل هذا النوع من أجهزة الليزر أخطار الحريق.

مأخوذ من : web.priceton.edu/sites/ehs/laserguide/sec2.htm;the royal school of artillery at www.atra.mod.uk/atra/rsabts/pdf/G-Electro-optics/G02-SAFE.pdf.Accessed March 22,2004

الجدول رقم (١٥-٢). تصنيف اللجنة الدولية للصليب الأحمر لليزر المستخدم في الحروب[١٤] .

الفئة أ	لم تصمم أنظمة هذه الأجهزة أساساً للاستخدام المضاد للأفراد، لكن في ظروف الحرب يمكن أن تحمل خطراً على العين.
الفرعية ١أ	تشمل أنظمة اكتشاف النطاق الليزري، وأنظمة تصميم وصناعة الهدف الليزري، أنظمة الرادار الضوئية (LIDAR). إن أغلبية أنظمة اكتشاف النطاق الليزري ليست آمنة للعين.
الفرعية ٢أ	وتشمل أنظمة التحري، التدريب، المحاكاة، والأنظمة المحمولة الصغيرة. من أمثلة هذه الفئة الفرعية الرؤية الليزرية الليلية / النهارية المقتطعة من ماسورة المسدس، حيث تظهر بقعة الضوء مكان ارتطام الطلقة.
الفئة ب	الأنظمة المضادة لأجهزة الاستشعار. صممت هذه الأنظمة بهدف إيجاد، وإغلاق، أو تدميرالرؤية البصرية للعدو، وإجراء مسح، ومعرفة النطاق، والتوجيه، وأنظمة الاتصالات.

obeikandl.com

تابع الجدول رقم (١٥–٢).

الفئة ج	الأنظمة المضادة للأفراد. وقد صممت هذه الأجهزة خصيصاً لإحداث الأذية الشخصية، والتي ستشمل أذية العين في هذه الحالة. وقد تم تصنيف كل المعلومات حول هذه الأجهزة. والاستثناء الذي يبين طبيعة هذه الفئة هو ليزر الرؤية المبهرة للبحرية البريطانية LDS. طبق هذا النظام في سفن تابعة للبحرية البريطانية واستخدم في حرب جزر الفوكلاند ١٩٨٢. من الهام أن ندرك أن الطاقة وطول الموجة لهما القدرة على إبهار العين على مسافة ٥كم وإلحاق العمى على مسافة كيلومتر واحد. تم تسويق موزع الليزر الصيني المحمول ٣٣-كغ ٨٧-zm في السوق الدولية كسلاح مضاد للجنود وأجهزة الاستشعار. ويبقى العالم الثالث السوق المستهدف لهذا النوع من السلاح الليزري.
الفئة د	الأنظمة المضادة للمواد. ويعتبر الليزر التكتيكي وأسلحة المبادرة للدفاع الجوي الأمريكي أمثلة عن هذه الأنظمة. لا تسبب هذه الأنظمة أذية للعين فقط بل يمكنها أن تقتل.

الشكل رقم (١٥–٨). الليزر التكتيكي عالي الطاقة (تركيب ثابت تحت الاختبار).

obeikandl.com

ويبين الجدول (١٥-٣) تفاصيل لأغلب المواد الليزرية أهمية والأنواع التي تقابلها من الليزر ويبقى هذا الجدول غير كامل. ويبين الصف المظلل طول الموجة الفعال لليزرات وحيدة اللون، بينما يبين الصف الأبيض الليزرات عديدة الألوان.

الجدول رقم (١٥-٣). أنواع الليزر.

	طول الموجة	الطاقة	نظام التشغيل	التطبيقات
الليزر ثنائي الصمام نصف الناقل Semiconductor diode laser				
ثنائية الصمام الوحيدة Single diodes	تحت حمراء إلى مرئية	١-١٠٠ ميغاواط	وضع مستمر ونبضي	الإلكترونيات البصرية: DVD، CD
قضبان الليزر الثنائية Diode laser bar	تحت حمراء إلى مرئية	حتى ١٠٠ واط	وضع مستمر ونبضي	مزود تدفق ضوئي لليزرات الصلبة
الليزر ذو الحالة الصلبة Solid-state laser				
ليزر ياغ Nd-YAG laser	١,٦ميكرومتر قرب تحت الحمراء	١واط-٣كيلوواط	وضع مستمر ونبضي	مواد العمليات، القياس، تطبيقات طبية
الليزر الياقوتي Ruby laser	حمراء	الكثير من الميغاواطات	وضع نبضي	القياس، السند الخطي النبضي
الليزر الغازي ليزر ثاني أكسيد الكربون CO2 laser	١,٦ميكرومتر تحت حمراء بعيدة	١واط-٤٠كيلوواط (١٠٠ميغاواط في النموذج النبضي)	وضع مستمر ونبضي	مواد العمليات، تطبيقات طبية، فصل النظائر

obeikandl.com

تابع الجدول رقم (١٥-٣).

	طول الموجة	الطاقة	نظام التشغيل	التطبيقات
ليزر الهيجان Excimer laser	١٩٣ نانومتر ٢٤٨ نانومتر ٣٠٨ نانومتر	١كيلوواط- ١٠٠ميغاواط	وضع نبضي ١٠-١٠٠ نانوثانية	التصنيع الدقيق، كيمياء الليزر، تطبيقات طبية
ليزر هيني HINI	غالباً ٦٣٢,٨ نانومتر	١ميغاواط- ١واط	وضع مستمر	القياس، السند الخطي
ليزر شاردة الأرغون Argon ion laser	غالباً ٥١٥٤٥٨ نانومتر	١ميغاواط- ١٥٠واط	وضع مستمر ونبضي	تقنية الطباعة، ضخ الليزر من أجل تنشيط ليزر الصبغة، تطبيقات طبية
ليزر الصبغة Dye laser	مستمر بين تحت الحمراء وفوق البنفسجية (صبغات مختلفة)	١ميغاواط- ١واط	وضع مستمر ونبضي	القياس، التحليل الطيفي، تطبيقات طبية

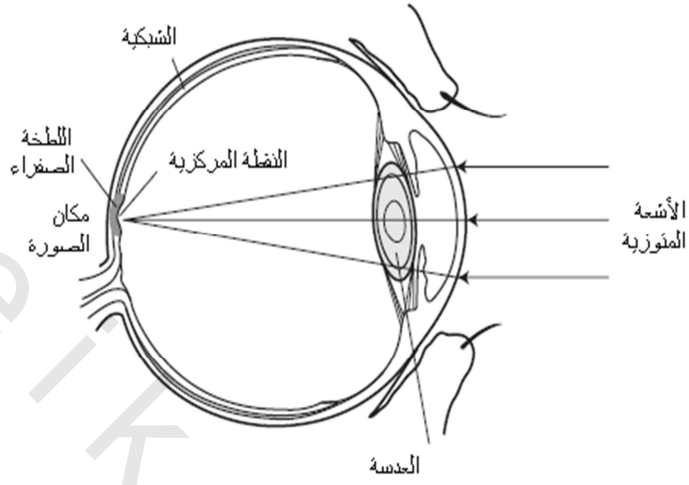
مأخوذ من: ILT- laser-tutorial.htm fraunhofer، ١٨ آب ٢٠٠٣

الأذيات العينية

العين هي جزء الجسم الأكثر عرضة لخطر الليزر. ويمكن أن يحدث الضرر العيني بمستويات طاقة أقل بكثير من مثيلاتها التي تؤثر على الجلد. وهذا الضرر إما أن يكون مؤقتاً وإما أن يكون دائماً، وهذا يعتمد على طول الموجة وطاقة الليزر. ولكون العين أكثر حساسية والحدقات تكون أكبر في الظلام، فإن الأسلحة الليزرية يكون لها تأثير أكبر في الليل عنه في النهار. عموماً، الأذيات العينية أكثر خطورة بكثير من الأذيات الجلدية. تقوم الأسلحة الليزرية بتكثيف الضوء والحرارة على الهدف.

واعتماداً على طاقة الليزر، يمكن لهذا الضوء أن يحرق الأجهزة البصرية أو أن يتسبب بعمى دائم عند مشغليها. إذا كان الشخص يستخدم جهازاً بصرياً بهدف الرؤية من خلاله مثل النظارات المكبرة، فإن قوة الشعاع تكبر وتتضخم وهذا يمكن أن ينتج أذية أكبر للعين. وحتى أجهزة الليزر المتواضعة يمكن أن تسبب العمى المؤقت لدى الشخص المعرض والذي ينظر من خلال المنظار. ويمكن استخدام أجهزة الليزر ذات الطاقة الأعلى بهدف تدمير الأشياء الموجودة في الطائرة أو التي على الأرض. إن العين البشرية جهاز بصري معقد. إنها مصممة لنقل وتركيز وكشف الضوء، حيث يمر الضوء عبر القسم الأمامي للعين من خلال القرنية. يتركز الضوء الذي يدخل في بقعة تقع خلف العين (الشبكية). ويشكل الضوء صورة على خلايا الشبكية التي صممت خصيصاً لكشف الضوء. تشكل القرنية الطبقة الشفافة الخارجية للعين. يمكن للقرنية أن تتحمل الغبار، التراب، والمخاطر البيئية الأخرى. تنمو خلايا القرنية بسرعة لترمم نفسها خلال ٤٨ ساعة وهذا يعني أن أذيات القرنية البسيطة تشفى بسرعة. الخلط المائي عبارة عن سائل لزج بين القرنية والعدسة. يقوم الماء الموجود في الخلط المائي بامتصاص الحرارة، وبذلك يحمي الأجزاء الداخلية للعين من الإشعاع الحراري. عدسة العين عبارة عن نسيج مرن يغير شكله بهدف تركيز الضوء على خلفية العين. عندما تقوم العدسة بتغيير شكلها، فإنها تسمح للعين بالتركيزعلى الأشياء القريبة والبعيدة. تتحكم القزحية بكمية الضوء التي تدخل العين. وهي الجزء الملون من العين الذي يضبط شدة الضوء وذلك بتقلصه أو توسعه. وتغير حجم القزحية هذا يضبط حجم الحدقة، والذي يتحكم بكمية الضوء التي تدخل العين. تعتبر الشبكية المنطقة الحساسة للضوء وتتوضع في القسم الخلفي للعين. وهي تحتوي على نوعين من خلايا المستقبلات الضوئية: " العصي والمخاريط ". تقوم هذه الخلايا بتحويل الصورة البصرية على الشبكية إلى إشارات كهربائية، ويقوم العصب البصري بحمل هذه الإشارات الكهربائية إلى الدماغ.

النقطة المركزية هي جزء الشبكية المركزي الأكثر حساسية، إنها منطقة الشبكية المسؤولة عن الرؤية المفصلة. وعندما تتأذى النقطة المركزية بإشعاع ليزري أو بأي سبب آخر، فإن الشخص يصبح أعمى رسمياً بسبب فقدانه الرؤية المفصلة. الخلط الزجاجي عبارة عن سائل هلامي عديم اللون يملأ المنطقة بين القزحية والشبكية. وهو لا يتجدد بمعنى لو حصل زربان لهذا السائل الهلامي من العين إلى خارجها فلن تستطيع العين إعادة إنتاجه، لذلك يمكن أن يقود أي انثقاب يسبب خسارة في الخلط الزجاجي إلى عمى دائم. تعتمد خطورة أذيات العين الليزرية على جرعة وموقع التعرض في العين. تعتمد جرعة التعرض للنسيج العيني على طبيعة الشعاع الليزري وطبيعة الجو الذي قطعه. وتشمل طبيعة الشعاع الليزري: الطاقة النبضية، مدة النبض، وطول موجة الليزر. ويؤثر الجو الذي مر به الشعاع الليزري على الطاقة المنتجة لليزر؛ وتشمل هذه العوامل الجوية: النطاق الجوي، محتوى الجو من الماء، الاضطرابات الجوية، والتلوث الجوي. إن شدة ضوء الشكل المتشكلة على الشبكية أكبر ١٠٠٠٠ مرة من شدة الضوء الذي تستقبله مقدمة العين. ويؤخذ هذا المكسب البصري بعين الاعتبار لأنه يشكل خطراً على العين مع دخول الشعاع الليزري إليها. (الشكل رقم ١٥-٩). ومع تعرض شخص ما إلى الضوء الليزري، فإنه قد يصاب بالعمى المؤقت (الانبهار) وربما يصاب بعمى طويل الأمد (التحليل الضوئي) أو أن يعاني من تغيرات دائمة في الوظيفة البصرية بسبب آفات أو نزوف بالشبكية). ويزداد احتمال إصابة العين مع استخدام الليزر في ظروف مفتوحة وخارجة عن السيطرة.



الشكل رقم (١٥–٩). تضخيم العدسات العينية لتأثيرات الإشعاع الليزري.

إن الشكاوي التي تتعلق بفقدان الرؤية أو ضعف الأداء البصري الذي يتسبب به ضوء الليزر الصادرعن الأجهزة الليزرية الهادفة أو أجهزة الليزر الترفيهية في الحفلات أو عروض الليزر في الهواء الطلق أصبحت أكثر شيوعاً. وقد تسبب هذا التعرض الليزري بإحداث العمى المؤقت لدى الطيارين على الخطوط الجوية التجارية سواءً في طائرات الهيليكوبتر أو الطائرات ذات الأجنحة الثابتة.[١٥-١٦]

المعالجة: لا توجد حالياً معالجة مقبولة لأذيات الليزر والضوء العينية. إن الأذية الليزرية العينية يمكن أن تسوء مع الوقت، لذلك يجب تقييم أي شخص يحتمل إصابته بأذية عينية ليزرية فور إصابته ومن ثم بفواصل منتظمة. إن المريض المصاب بأذية عينية ليزرية يعاني من ألم حاد بالعين، فقدان رؤية مفاجىء، رؤية متقطعة بقعية، أو عدم توجه. وتتباين أذية النسج العينية حسب طول موجة الليزر. وقد أدرجت أطوال موجات مختلف أنواع الليزر في الجدول رقم (١٥–٤) ويظل هذا الجدول بعيداً عن

الكمال بسبب تطوير ليزرات جديدة وبشكل يومي تقريباً. عموماً، يظهر الصف المظلل الموقع على طيف طول الموجة الليزرية. (الشكل رقم ١٥-١٠) تبين طيف الضوء وأماكن سقوط الأنواع المختلفة من الضوء حسب طول الموجة. تمتص الأشعة تحت الحمراء البعيدة والتي تتراوح بين ٣٠٠٠ نانومتر و١مم بواسطة القرنية (الشكل رقم ١٥-١١). ويمكن لليزر النبضي ذي الطاقة العالية أن يحرق أو يثقب القرنية بشكل خطير. وهنا يجب ألا يجري تطعيم هذه الحروق والانثقابات الشديدة، كما يجب حماية العين كي لا يحصل زربان خارجي للخلط الزجاجي. كما يمكن علاج الحروق الليزرية البسيطة عن طريق تغطيتها بضماد خاص وتطبيق المضاد الحيوي العيني المناسب. يمكن للعدسة أن تمتص بعض الأشعة تحت الحمراء بطول موجة IR-A يتراوح بين ٧٠٠-١٤٠٠ نانومتر وطول موجة IR-B يتراوح بين ١٤٠٠-٣٠٠٠ نانومتر. ويعتبر الإشعاع المرئي بطول موجة IR-A أكثر خطورة ويتم نقله عن طريق الأقسام البصرية للعين. لتصل بالنهاية إلى الشبكية، حيث تقوم الظهارية الصباغية في الطبقة الشبكية والمشيمية بامتصاص أغلب الأشعة. أما المشيمية فهي طبقة بلون بني غامق وبشكل استثنائي تحتوي على أوعية دموية كبيرة ونسبة جريان دموي كبير. لا تتطلب حروق الشبكية الليزرية أي ضماد عيني لأنه بالواقع قد ينقص ما تبقى من الرؤية عند الشخص. إن أذية الشبكية أو النزف الناتج عن أذيتها يمكن يسبب فقدان بصر تام. إن الشخص الذي يرى بقعاً مظلمة كبيرة في مركز الرؤية أو بالقرب منه، أو الذي لديه شيء عائم في العين، أو الذي لديه تجمع دموي بالعين يجب نقله إلى المشفى مباشرة وتقديم الدعم العيني. يجب معالجة النزف داخل العين بوضع رأس المريض عالياً من أجل السماح للدم بالتوضع في القسم السفلي للعين. انظر إلى (الصور الملونة ١٥-١ و١٥-٢ و١٥-٣ التي تصور أذيات العين الليزرية).

الجدول رقم (١٥–٤). أطوال موجات الليزر.

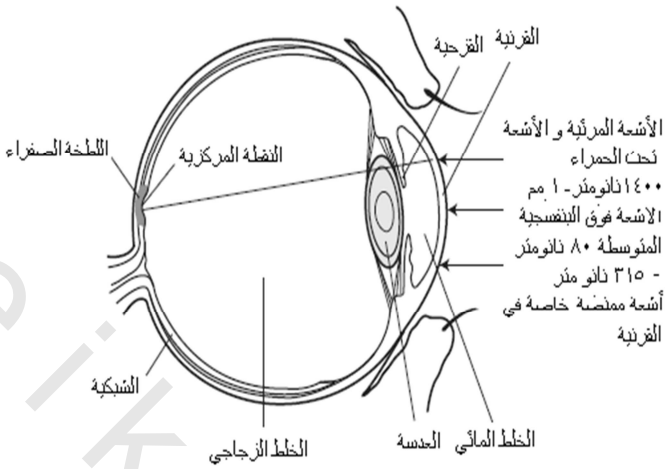
الوسط الليزري	نوع الليزر	حول الموجة
	تحت الحمراء البعيدة	
Co2 ثاني أكسيد الكربون	غاز	١٠,٦٠٠ نانومتر
	تحت الحمراء	
HENE هي ني	غاز	١,١٥٢ نانومتر
Argon أرغون	غاز – شاردي	١,٠٩٠ نانومتر
ND-YAG ن- د ياغ	الحالة الصلبة	١,٠٦٤ نانومتر
In GaAs إن جا فز	الصف نقل	٩٨٠ نانومتر
Krypton كريبتون	غاز – شاردي	٧٩٩,٣ نانومتر
CR: LiSAF سي آر : ليساف	الحالة الصلبة	٧٨٠- ١,٠٦٠ نانومتر
GaAs/GalAs جا الس/ جا الس	الصف نقل	٧٨٠- ٩٠٥ نانومتر
Krypton كريبتون	غاز – شاردي	٧٥٢,٥ نانومتر
Ti: Sipphire تي : سبهاير	الحالة الصلبة	٧٠٠- ١٠٠٠ نانومتر
	الضوء المرئي	
Ruby الياقوت	الحالة الصلبة	٦٩٤ نانومتر
Krypton كريبتون	غاز – شاردي	٦٧٦,٤ نانومتر
In GaAlp إن جالب	الصف ناقل	٦٣٥- ٦٦٠ نانومتر
HENE هي ني	غاز	٦٣٣ نانومتر
Ruby الياقوت	الحالة الصلبة	٦٧٨ نانومتر
HENE هي ني	غاز	٦١٢ نانومتر
HENE هي ني	غاز	٥٩٤ نانومتر
Cu سي يو	بخار معدني	٥٧٨ نانومتر
Krypton كريبتون	غاز – شاردي	٥٦٨,٢ نانومتر
Hene هي ني	غاز	٥٤٣ نانومتر
DPSS دي بي ا س اس	الصف ناقل	٥٣٧ نانومتر

obeikandl.com

تابع الجدول رقم (١٥-٤).

الوسط الليزري	نوع الليزر	حول الموجة
Krypton كريبتون	غاز – شاردي	٥٣٠,٩ نانومتر
Argon ارغون	غاز – شاردي	٥١٤,٥ نانومتر
Cu سي يو	بخار معدني	٥١١ نانومتر
Argon ارغون	غاز – شاردي	٤٥٧,٩ نانومتر وغيره الكثير
HeCD هي سي دي	غاز – شاردي	٤٢٢ نانومتر
+N2 ن٢+	غاز	٤٢٨ نانومتر
Krypton كريبتون	غاز – شاردي	٤١٦ نانومتر
	تحت البنفسجية قريبة	
XeF إكسي إف	غاز (هيجان)	٣٥١ نانومتر (فوق البنفسجية – أ)
N2 ن٢	غاز	٣٣٧ نانومتر (فوق البنفسجية – أ)
XeCl إكسي سي ال	غاز (هيجان)	٣٠٨ نانومتر (فوق البنفسجية – ب)
	تحت البنفسجية بعيدة	
KrF كر اف	غاز (هيجان)	٢٤٨ نانومتر (فوق البنفسجية-سي)
Argon SHG ارغون اس اتش جي	غاز – شاردي/ بلورات ب ب و	٢٢٩ نانومتر (فوق البنفسجية-سي)
KrCl	غاز (هيجان)	٢٢٢ نانومتر (فوق البنفسجية-سي)
ArF	غاز (هيجان)	١٩٣ نانومتر (فوق البنفسجية-سي)

obeikandi.com



الشكل رقم (١٥–١٠). الطيف البصري. ضوء الليزر غير المتشرد ويشمل نطاقاً من الأشعة فوق البنفسجية بين (١٠٠–٤٠٠ نانومتر)، وأشعة مرئية (٤٠٠–٧٠٠ نانومتر)، وأشعة تحت الحمراء (٧٠٠ نانومتر– ١ ملم).

الشكل رقم (١٥–١١). أطوال الموجات التي تؤذي القرنية.

obeikandl.com

حروق الجلد

إن إمكانية حدوث الأذية الجلدية الليزرية أكبر من الأذية العينية بسبب توفر نسيج جلدي أكبر بكثير من النسيج العيني. وعلى كل حال، تبقى الأذيات الجلدية الليزرية أقل خطورة من الأذيات العينية. ويبقى هذا الشيء جزئياً لأن الأذيات الجلدية لا تنتج عادة العواقب الوخيمة التي تعقب الأذيات العينية، وأيضاً لأن العين تقوم بتركيز الإشعاع الليزري كما ذكر سابقاً. تقع الأذيات الجلدية الليزرية مبدئياً ضمن مجموعتين: أذية حرارية (حروق) بسبب التعرض الحاد لإشعاعات الليزر عالية الطاقة، وأذية ضوئية بسبب التعرض طويل الأمد للإشعاع الليزري فوق البنفسجي المنتشر.

١- **الأذية الحرارية**: يمكن أن تنتج من اتصال مباشر مع الشعاع أو انعكاسات الليزر بالمرآة. عادة لا تكون هذه الأذيات خطيرة (مع أنها مؤلمة) ومن السهل تجنبها من خلال توفير التدبير المناسب للإشعاع والتوعية لأخطاره.

٢- الأذية الضوئية: يمكن أن تحصل مع الوقت بسبب التعرض المباشر للأشعة فوق البنفسجية أو انعكاساتها بالمرآة، أو حتى انعكاسات الليزر المبعثرة. ويتراوح تأثيرها من حروق شمسية بسيطة إلى خطيرة. علماً أن التعرض طويل الأمد قد يؤهب لحدوث سرطان الجلد. وقد يكون من الضروري استعمال ضماد يحمي العين وثياب وقائية للسيطرة على تأثير الأشعة فوق البنفسجية على العين والجلد. تصيب الأذيات الجلدية عادة الطبقة الخارجية الميتة من البشرة. وحتى الأذيات التي تخترق الجلد، تشفى بسرعة. تحصل أكثر أذيات الجلد الليزرية بسبب أطوال الموجات تحت الحمراء البعيدة كالتي تنتجها ليزرات ثاني أكسيد الكربون. كما يمكن أن تحدث الأذيات الجلدية بواسطة أطوال الموجات تحت الحمراء القريبة أو المرئية، لكن تتطلب حدوث هذه الأذية الضوئية شدة ليزرية أعلى من أطوال الموجات تحت الحمراء البعيدة.

(يعكس الجلد معظم أطوال الموجات تحت الحمراء القريبة أو المرئية ويقوم بامتصاص أطوال الموجات UVB-UVC). ويمكن للشعاع الليزري ضمن الطيف الضوئي وبأي طول موجة، مع طاقة ومدة كافية، أن يخترق الجلد ويسبب أذية داخلية عميقة. يكون الألم الناتج من الأذية الحرارية الذي يسببه أغلب أنواع الليزر الهدفية كافياً لتنبيه الضحية للتحرك خارج مسار الإشعاع. ولسوء الحظ، تستخدم حالياً عدد من الليزرات عالية الطاقة والمرئية وتحت الحمراء في الصناعة. تستطيع هذه الأنواع من الليزر إنتاج حروق جلدية هامة في أقل من ثانية.

التهديد

يعتبر الليزر سلاح الطاقة الموجه الوحيد الذي تطرحه حالياً الولايات المتحدة والقوات العسكرية الأخرى. في حالات كثيرة، ليس المقصود من الليزر أن يكون سلاحاً بحد ذاته، بل هو جهاز استهداف لسلاح آخر، مثل الصواريخ أو القنابل الذكية. وتناسب خصائص الليزر هذا الهدف جزئياً. وقد طورت جيوش عدة دول أنواع من أجهزة الليزر لاستعمالها لكشف النطاق وتصميم الأهداف، فعندما كان نطاق الليزر ضعيفاً جداً، تم تطوير ليزر ذي طاقة عالية من أجل إضاءة الهدف. هنالك مشكلة محتملة في العديد من أجهزة الليزر العسكرية، حيث يمكنها أن تسبب أذية شبكية العين لأي شخص ينظر إلى الشعاع الليزري، حتى على مسافة عدة أميال. وسرعان ما يصبح هذا الشيء ميزة عندما يدرك الجيش أن الليزر يمكن استعماله بفعالية بهدف التعطيل الشخصي عن طريق إصابة الشخص بالعمى أو بالانبهار. في عام ١٩٨٥م، طورت البحرية البريطانية سلاحاً غير مصنف يركب في السفن التي تغادر خارج البلاد ويهدف إلى إصابة طياري العدو القادم بالعمى وذلك ضمن نطاق يصل إلى ثلاثة أميال. وقد تم صنع آلاف من أجهزة الليزر ذات النطاق البعيد وأخرى ذات القدرة على تحديد الهدف كما تم تزويد كثير من قوات الدول بها. وكذلك، يمكن لهذه

الأجهزة أن تجد طريقها إلى أيادي الإرهابيين لكي يطبقوها ضد المدنيين في الولايات المتحدة. هذا ويمكن استخدام أجهزة ليزر مدنية أخرى وتطبيقها بسهولة لأهداف مماثلة. في الواقع، استخدم قاطعو الطرق في إنكلترا مؤشرات ليزرية بسيطة لإصابة الضحية بالعمى قبل سرقتها.[١٧] وقد سجلت التقاريرحدوث ألم بالعين وصداع لمدة عدة أسابيع بعد تعرض العين العابر لإشعاعات المؤشرات الليزرية.[١٨] (يصعب فهم هذا الشيء، لأن الألم المستمر ليس نتيجة شائعة للعلاج الليزري في الداء السكري، حيث تتعرض الشبكية إلى مقادير كبيرة من الطاقة الليزرية).[١٩-٢٠] وقد استخدم الإرهابيون الليزر في محاولة لإصابة طياري المروحيات بالعمى. وليس مستبعداً أن يستخدم الإرهابيون الليزر القوي نسبياً في الشاحنات أو السيارات في محاولة لإصابة الطيارين الآخذين بالهبوط في المطارات التجارية بالعمى.[٢١] وبشكل مشابه، قد تستخدم أجهزة الليزر البسيطة لتدمير الرؤية عند المسؤولين عن تطبيق القانون وذلك في إطار الهجمات الإرهابية. من غير الوارد أن يطبق الإرهابيون أجهزة الليزر الفئة ٣ب أو ٤. لكن يبقى هذا الشيء ممكناً. يجب أن يكون مقدمو الخدمات الطبية الإسعافية وعلى جميع المستويات جاهزين لمعالجة الأذيات العينية الناتجة عن أجهزة الليزر الفئة ٢ أو ٣، كون هذه الأذيات نادراً ما تحدث خلال حياة المدنيين بعيداً عن تدخل الإرهابيين.

الحماية

لاتوجد إجراءات مضمونة مضادة للعمى الذي يسببه الليزر. وكل من هذه الجهود الوقائية التالية سوف تعيق القدرة على الرؤية وعلى تنفيذ الأنشطة التي تتطلب الرؤية.

١- التجنب

لا يمر الشعاع الليزري خلال الأشياء غير الظليلة، فأي غطاء غير ظليل يمكن أن يزودنا بالحماية ضد كل الإشعاعات عدا أجهزة الليزر الفئة الرابعة. تجنب النظر

المباشر نهائياً باتجاه أي شعاع ليزري أو انعكاساته لو أمكن ذلك، علماً أن الانعكاسات على السطوح اللامعة يمكن أن تسبب الأذية رغم وجود التغطية الأمامية.

٢- التغطية

يمكن أن يؤمن تطبيق غطاء عيني على العين حماية جزئية من الليزرات المسببة للعمى. ولسوء الحظ، يمكن لهذا الغطاء أن يحرم حامله من الإدراك العميق والرؤية المحيطية. عموماً، استخدام الغطاء العيني يمنع العمى فقط في العين المغطاة.

٣- التصفية

تعتبر هذه الطريقة من الحماية ضد التهديد الليزري بسيطة تماماً، اصنع زوجاً من النظارات الشمسية الوقائية التي تعكس ضوء الليزر وتسمح لأطوال الموجات الأخرى بالعبور، وبذلك يمكن لحامله أن يرى. كما أن أقنعة الخوذة والنظارات الواقية يمكنها منع الإشعاع الليزري من أذية عيون مستخدميها. يمكن لكل ما سبق أن يؤدي عملاً حسناً لو تمكنا من تحديد التهديد الليزري مسبقاً وأن يكون هذا التهديد الليزري محدوداً بأطوال موجات واحدة أو اثنتين. وكالعادة، يكشف البحث الدقيق الذي يقوم به الإرهابي المعدات الوقائية المتاحة حالياً لموظفي المؤسسة العسكرية، والمسؤولين عن تطبيق القانون، ومقدمي الخدمات الطبية الإسعافية. ومع توفر هذه المعلومات، يمكن للإرهابي أن يختار طول موجة ليزر لا يوجد حماية لها. بالإضافة إلى أن مستوى الحد من الأذية التي توفرها الأقنعة المتاحة حالياً تكفي فقط ضد الطاقات الليزرية المتوفرة في الوقت الحاضر وقد لا تكون كافية ضد الليزرات السوفيتية والصينية والكورية الشمالية أو الباكستانية ذات الطاقة العالية والتي يمكن استخدامها كأسلحة مضادة للأفراد. ومن المتوقع أن يطور قريباً تهديد الليزر الانضباطي (ذو تردد مرن). إن استخدام النهج التقني في الحماية ضد الليزرات ذات التردد الثابت لا يمكن تطبيقه في الحماية ضد التهديد المرن ولا حتى في الحماية من عدد كبير من التهديدات ذات التردد الثابت. ومع

بناء مصافي رفض الشريط على شكل السندوتش، تنقص قابلية النقل في الأقنعة على أطوال الموجات الأخرى أيضاً، مما يجعلها غير صالحة للاستعمال في الليل ومحدودة الفائدة في أوقات النهار.

يجب التشديد على تطبيق الوسائل الوقائية حتى تكون فعالة، يجب وضع نظارات الوقاية من الليزر قبل التعرض إلى الليزر، ويجب أن تمتلك هذه الوسائل الوقائية خصائص رفض التردد المناسبة لليزر المستعمل. هذا يشكل مشكلة صعبة بالنسبة للمسؤولين عن تطبيق القانون ومقدمي الخدمات الطبية الإسعافية الذين قد يواجهون أياً من أجهزة الليزر هذه في حالة التهديد الإرهابي.

بواعث إشعاع الموجات الدقيقة
Microwave Radiation Emitters

تم تغطية موضوع بواعث إشعاع الموجات الدقيقة والتأثيرات على الأجهزة في فصل سابق " الأسلحة الكهرومغناطيسية النبضية ". يمكن أن ينتج عن التعرض المديد لمولدات الموجات عالية الطاقة الدقيقة تأثيرات فيزيائية ونفسية عند الإنسان تشمل الاحساس بالسخونة والصداع والتعب العام والضعف والدوار. وتعتمد شدة هذه التأثيرات على الطاقة الناتجة عن السلاح والمسافة بين مولد الطاقة والشخص.

مولدات الشعاع الجزيئي
Particle Beam Generators

شعاع الجزيئات عبارة عن تدفق جزيئات ذرية أو تحت ذرية. وهذه الجزيئات عالية الطاقة، وعندما تتركز في الشعاع، يمكنها أن تصهر أو أن تكسر المعادن والبلاستيك. ويمكنها أيضاً توليد أشعة سينية في نقطة التصادم. هذه الأسلحة لاتزال في مرحلة التطوير فقط ومن المرجح أن تكون في منأى عن أيادي الإرهابيين.

الجدول رقم (١٥–٥). تأثيرات أجهزة الليزر الشائعة.

نوع الليزر	الشبكية	العدسة	القرنية	الجلد	عملية التأثير حيوي	طول الموجة نانومتر
CO2	–	–	أذية حرارية	×	حراري	١٠٦٠٠
HFl	–	–	أذية حرارية	×	حراري	٢٧٠٠
Erbium-YAG	–	ساد نافخي الزجاج	أذية حرارية	×	حراري	١٥٤٠
Nd:YAG[a]	أذية شبكية	ساد نافخي الزجاج	أذية حرارية	×	حراري	١٣٣٠
Nd:YAG	أذية شبكية	×	×	×	حراري	١٠٦٠
Gas (diode)	أذية شبكية	×	×	[b]	حراري	٧٨٠– ٨٤٠
He – Ne	أذية شبكية	×	×	[b]	حراري	٦٣٣
Ar	أذية شبكية	×	×	×	حراري + ضوئي	٤٨٨– ٥١٤
XeFl	أذية شبكية[c]	×	التهاب قرنية ضوئي (فلاش ويلدر)	×	ضوئي	٣٥١
XeCl	أذية شبكية	×	التهاب قرنية ضوئي (فلاش ويلدر)	×	ضوئي	٣٠٨

مأخوذ من: web.priceton.edu/sites/ehs/laserguide/sec2.htm;the royal school of artillery at www.atra.mod.uk/atra/rsabts/pdf/G-Electro-optics/G02-SAFE.pdf.Accessed March 22,2004

[a] أطوال الموجات ١٣٣٠٠ نانومتر (طيف تحت حمراء بعيد جداً) أو أكثر شائعة في بعض أنواع الليزر Nd:YAG والتي أظهرت تأثيرات آنية على القرنية، العدسة، الشبكية وذلك في دراسات الأبحاث البيولوجية. [b] مستويات الطاقة لهذه الأنواع من الليزر عادة تكون غير كافية لإحداث خطورة جلدية هامة. [c] تسيطر التأثيرات الضوئية بسبب التعرض طويل الأمد للشبكية (وقت التعرض أكثر من ١٠ ثانية) تشكل أطوال الأمواج المرئية وتحت الحمراء القريبة خطورة جزئياً خلال انتقالها خلال الوسائط العينية، حيث تتركز في بقعة على الشبكية بقطر ١٠–٢٠ ميكرومتر. وبذلك تكون شدة مثل هذا الضوء على الشبكية ١٠٥ أضعاف شدته على القرنية. ويمكن أن يعزز التركيز الذاتي لنبضات بطول فيمتو– ثانية في العين كثافات شبكية العين بشكل أكبر. وبالتالي، يقل مستوى عتبة إصابة الشبكية عن عتبة إصابة القرنية..

obeikandl.com

المراجع

1. Conway M: Reality bytes: Cyberterrorism and terrorist 'use' of the internet. *First Monday*, http://www.firstmonday.dk/issues/issue7_11/conway/ (Accessed July 4, 2003).
2. Title 22, US Code, § 2656f(d)2.
3. Jesdanun A: Cybercafes pose security problems. CBSNews.com. http://www.cbsnews.com/stories/2003/07/22/tech/main564568.shtml (Accessed March 20, 2004.)
4. Cyber war! The warnings? "Frontline." PBS, April 24, 2003 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/ (Accessed April 28, 2003).
5. Cyber war! Introduction. "Frontline." PBS, April 24, 2003 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/synopsis.html (Accessed April 28, 2003).
6. Cyber war! Introduction, "Frontline." PBS, April 24, 2003 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/ etc/synopsis.html (Accessed April 28, 2003).
7. Cyber war! Introduction, "Frontline." PBS, April 24, 2003 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/ etc/synopsis.html (Accessed April 28, 2003).
8. Saltus, R: Blackout led to weapon that darkened Serbia. *Boston Globe*, May 4, 1999:A27.
9. Izakovic (NI): Conventional electromagnetic pulse warheads. Deepspace4, http://www.deepspace4.com/pages/science/mp/empwarheads.htm (Accessed March 26, 2003).
10. Amos D: Police chase psychology. *ABCNews.com*, http://abcnews.go.com/onair/ CloserLook/wnt000713_CL_policechase_feature.html (Accessed April 15, 2003).
11. Rogers K: Are electromagnetic pulses terrorists' next weapon of choice? *Las Vegas Review-Journal*, September 1, 2001, http://www.globalsecurity.org/org/news/ 2001/010930-attack04.htm (Accessed March 26, 2003).
12. Sample I: Just a normal town... *New Scientist*, http://www.newscientist.com/ nl/0701/end.html (Accessed August 17, 2003).
13. Sample I: Just a normal town... *New Scientist*, http://www.newscientist.com/nl/ 0701/end.html (Accessed August 17, 2003).
14. Doswald-Beck L (ed): *Blinding Weapons: Report of the Meeting of Experts Convened by the International Committee of the Red Cross on Battlefield Laser Weapons, 1989–1991*. Geneva, Switzerland, International Committee of the Red Cross, 1993.

15. Kurtzweil P: Investigators' reports: Laser light shows nixed until fixed. US Food and Drug Administration, http://www.fda.gov/ fdac/departs/496_irs.html (Accessed August 21, 2003).
16. Coleman, J: Assembly panel approves laser pointer bill. *Las Vegas News*, May 08, 1999, http://www.lvrj.com/cgi-bin/printable.cgi?/lvrj_home/1999/May-08-Sat-1999/news/11141492.html (Accessed August 21, 2003). *Adapted from:* http://web.princeton.edu/sites/ehs/laserguide/sec2.htm; Laser safety at http://web.princeton.edu/sites/ehs/laserguide/sec2.htm; Laser safety background at http://www.femto.sims.nrc.ca/LaserSafety/lsafety7.htm; The Royal School of Artillery at www.atra.mod.uk/atra/rsabst/pdf/G-Electro-Optics/G02-SAFE.pdf. Accessed March 22, 2004.
[a] Wavelengths of 13,300 nm (very far-infrared spectrum) or more are common in some Nd:YAG lasers and have demonstrated simultaneous cornea/lens/retina effects in biological research studies.
[b] Power levels of these lasers are not normally sufficient to be considered a significant skin hazard.
[c] Photochemical effects dominate for long-term exposures to the retina (exposure times of more than 10 seconds). Visible and near-infrared wavelengths are particularly hazardous since they are readily transmitted through ocular media and are focused to a spot on the retina 10–20 _m in diameter.
Thus the intensity of such light at the retina will be on the order of 105 times greater than at the cornea. Self-focusing of femtosecond pulses within the eye can further enhance retinal intensities.Hence, retinal damage thresholds are several orders of magnitude lower than those for corneas.
17. Anonymous: Killer pens. *Newsweek*, November 24, 1997:8.
18. Seeley D: *Laser point causes eye injuries?* Orlando, FL, Laser Institute of America, 1997.
19. Mainster MA, Sliney DH, Marshal J, et al: But is it really light damage? *Ophthal* 1997;104:179-190.
20. Yolton RL, Citek K, Schmeisser E, et al: Laser pointers: Toys, nuisances, or significant eye hazards? http://www.opt.pacificu. edu/journal/Articles/archives/ laserpaper.html (Accessed August 20, 2003).
21. Anonymous: Russian ship's laser caused eye injury, Navy officer says. http://www.aeronautics.ru/nws002/ap036.htm (Accessed August 21, 2003).