نطاق الفضاء الإلكتروني في الشرق الأوسط – إيران / سوريا / إسرائيل

بقلم جيف باردين، Treadstone 71 سبتمبر 2016

نطاق الفضاء الإلكتروني في الشرق الأوسط تنفجر بصورة هائلة مثل انفجار البيئة الطبيعية الحالية فيه. الفضاء الإلكتروني يعج بالتغيير المستمر. جهات التهديد الفاعلة الجديدة، والملاجئ الافتراضية الآمنة وزيادة مشاهدات المتطرفين تستدعي حماية النطاقات الافتراضية الآمنة.

ظهور شبكات التواصل الاجتماعي في الشرق الأوسط يوفر طريقة فاعلة في الوقت الفعلي لأعمال الدعاية، وسيطرة وتحكم غير منظم. وهو غير منظم لأن الأداة التي نختارها هي شبكات التواصل الاجتماعي. يقوم مستخدمو أدوات شبكات التواصل الاجتماعي مثل تويتر وفيسبوك بإنشاء حسابات مع قبول المتابعين أو الأصدقاء الذين يتطلبون معرفة مسبقة بأشياء محددة أو إمكانية الدخول على الدوائر المغلقة بناءً على السمعة. وقد ظهرت هذه الطريقة بجلاء أثناء ثورات الربيع العربي التي امتدت من شمال أفريقيا وحتى دول الخليج.

أدت العديد من أجهزة الدخول على الإنترنت بالإضافة إلى العديد من طرق نشر المعلومات إلى طرق جديدة كلياً لنشر المعلومات في الشرق الأوسط. هذه الطرق تفوقت على مراكز الدعاية الحكومية ومنافذ السيطرة على المعلومات. وتغلبت على الوسائل التي منعت حرية الرأي والتعبير. وقضت على مخاطر اكتشاف وسائل التواصل المتاحة من وجهة نظر الجهات التي حرمت هذه الوسائل.

وازدهرت وسائل التواصل المتاحة وأيضاً أتيحت الفرصة للمتطرفين لعرض وجهات نظرهم وآرائهم. هذه الآراء كانت حبيسة منذ أمدٍ بعيد في زنازين قذرة إلا أنها تطورت ونمت عبر سنوات من التخطيط. الشيء المميز في هذا التخطيط هو الإقبال على التواصل الحر المفتوح المحمي بسرية وخصوصية وبسرعة الإنترنت. تستغل وكالات الاستخبارات في الشرق الأوسط شبكات التواصل الاجتماعي كنتيجة للربيع العربي. وقد أصبحت شبكات التواصل الاجتماعي هي الآمر والمسيطر ووسائل التواصل وأجهزة كمبيوتر واستخبارات ورصد ومراقبة واستطلاع واستكشاف (C4ISR) للمُضْطَهَدين (مجلة تقنية الدفاع، 2011).

تعمل مواقع شبكات التواصل الاجتماعي مثل فيسبوك وتويتر كأسلحة في حروب الاتصالات والدعاية. لأن التواصل عبر هذه الوسائل هو رأس الحربة في الحشد والاستنفار والتطرف والتخطيط. يمكن النظر لهذه الأسلحة جميعها على أنها مخاطر وتهديدات.

حاولت الحكومات في جميع أرجاء الشرق الأوسط في البداية منع استخدام هذه الأسلحة لكنها غيرت منهجها وطريقتها.

ظهر بعدُ جديد في المفهوم والمعتقد في صورة مواقع التواصل الاجتماعي التي أصبحت أهدافاً للتجسس والاختراق. حكومات الشرق الأوسط تخترق في الوقت الحالي مواقع شبكات التواصل الاجتماعي بطرق تهدف إلى اختراق ومنع وإعاقة التواصل والاتصالات والتخطيط للأنشطة. يمكن تلخيص منهج التعامل مع الفضاء الإلكتروني بصفة عامة كانعكاس مباشر للاضطرابات الحادثة في الشرق الأوسط والناتجة عن سنوات من الدكتاتورية أدت إلى الكبت والقمع الاضطهاد والاستبداد.

تطور استراتيجيات الفضاء الإلكتروني – في سوريا وإيران

على عكس العوائق المالية الضخمة في بناء الجيوش والقوات البحرية والقوات الجوية يمكن اعتبار تنامي وسائل الحرب عبر الفضاء الإلكتروني كوسيلة منخفضة التكاليف نسبياً. كما أنه ليست هناك حاجة لإرسال القوات والجيوش. يمكن أن تكون الأهداف مجزئة بطبيعتها. ليست هناك حاجة لضرب دولة أخرى بالقنابل، فقد تكون النتائج محرجة على المستوى السياسي، إلا أن النتائج فعالة جداً وتترك الهدف يتساءل عما سيصيبه لاحقاً. التركيز الأساسي على المعرفة الفنية والتقنية ورغبة فطرية شديدة نحو الفضول المعرفي والاستكشاف كنقطة بداية لبناء قاعدة إستراتيجية حروب الفضاء الإلكتروني. أتت عملية التطور الحالي بعد هيكلة أولية غير منظمة نضجت و تحولت بالفعل إلى نموذج منظم وفاعل مدعوم أكاديمياً ومن الحكومات:

1. إمكانية الدخول على الإنترنت
2. تجربة واستكشاف الثغرات في مواقع الأعداء والخصوم
3. القرصنة كوسيلة بدائية مع التشويه العشوائي
4. التطوير المستمر لمهارات القرصنة والانتقال لمرحلة تهريب البيانات
5. المؤسسات ذات البناء الهش القائم على التعاليم القومية
6. المشاركة في القضاء على الأنشطة المميزة
7. تأسيس عدد محدود من شركات أمن الفضاء الإلكتروني
8. وضع المؤسسات الأكاديمية لمناهج تعليم دفاعية وهجومية
9. عقد مؤتمرات لأمن الفضاء الإلكتروني على المستوى المحلي

10. الاستهداف الصريح والمعلن على مستوى العالم للأعداء بناءً على وجهات نظر سياسية ودينية
11. وضع الحكومات لبرامج دفاعية في الفضاء الإلكتروني (للدفاع عن نفسها)
12. وضع الحكومات لبرامج حكومية في الفضاء الإلكتروني (للهجوم على الأعداء)
13. دمج المؤسسات ذات التركيب الهش مع الكيانات الحكومية والمؤسسات الأكاديمية
    a. استخدام المؤسسات ذات التركيب الهش كوكلاء لاستهداف الأعداء بناءً على
    b. أولويات الحكومة في متطلبات الاستهداف
    c. المؤسسات الافتراضية الخارجية التي تعكس وكلاء فعليين
14. توسيع المؤسسات الأكاديمية للمناهج التعليمية على مستوى شهادات الماجستير
15. استحواذ المؤسسات الأكاديمية على الألعاب المميزة
16. القيام بإجراءات فاعلة في الفضاء الإلكتروني ضد الأعداء أثناء فترات الاضطرابات الدينية والسياسية أو انخراط الجيش كأداة في السياسة الخارجية
17. إعلان الحكومة لأمن الفضاء الإلكتروني كواجب قومي ووطني

البحث عن الثغرات واكتشافها هو الإغراء الذي يفتح الشهية. بمجرد إيجاد هذه الثغرات يجب اختبار وتقييم المهارات الجديدة التي تم اكتشافها وتوسيعها لكي تصبح مهارات يمكن توثيقها وتكرارها وتكييفها. إمكانية تكييفها نظراً لسرعة التغيير في شبكات مواقع التواصل الاجتماعي وأمن مواقع الأعداء على الإنترنت يتطلب التعلم والتغيير المستمر للأساليب والتقنيات والإجراءات (TTPs). أثبتت سوريا وإيران أن الإجراءات السابق ذكرها فعالة من خلال تشكيل الجيش السوري الإلكتروني (SEA) (وحدة البرمجة في الجيش السوري الإلكتروني، 2014) ومجموعة أشيان للأمن الرقمي (Ashiyane Digital Security Group) (أشيان 2014) ولا يمكن تجاهل مجموعات أخرى مثل فريق أمن قراصنة مدينة بابل الإيرانية، والمخترقون الإيرانيون ورابطة القراصنة الإيرانيين والفريق الإيراني المدمر والمخرب (سميث 2006)، والفريق السوري للبرامج الضارة والخبيثة (مونكاستر، 2014). ورغم اختلاف الطرق التي اتبعتها المجموعتان إلا أن المجموعتين أتبعتا مساراً يعمل على دمجهما مع الحكومة والمؤسسات الأكاديمية. بدافع الضرورة والدافع الوطني ما دفعهما إلى السير مع الحكومة. اندمجت المجموعتان مع المؤسسات الحكومية المعنية.

دمجت إيران برامج الحرب الإلكترونية في الأنشطة العسكرية. وقد حاول كل من الحرس الثوري الإيراني (IRGC) والجيش عقد اتفاق مع الولايات المتحدة لزيادة قدرات تجميع الإشارات والاتصالات والاستخبارات. يقومون بذلك من خلال الاستخدام المكثف للألياف الضوئية المدفونة والاتصالات المؤمنة وتطوير المزيد من الطرق الآمنة لاستخدام الإنترنت وخطوط الاتصالات الأرضية (كوردسمان، 2007). تعمل جامعتا الحسين والشريف من أجل الوصول إلى "شبكة اتصالات إنترنت داخلية لا يمكن اختراقها (كوردسمان، 2007)." تزعم إيران أن هذا النظام قد تمت تجربته ميدانياً أثناء مناورات ولاية اقتدار في فبراير 2007 (الاستخبارات الأمريكية، 2007).

وقد اعتبر التعليم كأولوية قصوى في الخطط التنموية في البلاد؛ وقد سعت السلطات إلى زيادة معدلات الالتحاق بالتعليم الابتدائي (ماسلين، 2013). في الواقع ارتفعت معدلات التحاق الإيرانيين بالجامعات الأمريكية بنسبة 25% لتصل إلى 8700 طالب مقارنةً بزيادة نسبتها 25.65 لطلاب الدول الأخرى في الشرق الأوسط (ماسلين، 2013). أدى زيادة الانتباه للتعليم العالي إلى زيادة أعداد علماء الحاسوب ومهندسي التكنولوجيا وهما العنصران اللازمان لامتلاك برنامج أسلحة فضاء إلكتروني متطورة (كارول، 2008).

من المعروف أن مجموعة إيرانية أخرى هي الجيش الإيراني للفضاء الإلكتروني، قد وردت عنها تقارير تربطها بالهجمات التي جرت في الماضي على المؤسسات الغربية. ليس من المعروف في العلن أن للحرس الثوري الإيراني سيطرة على هذه المجموعة إلا أن العديد من القادة الإيرانيين قد أعلنوا عن مجهوداتهم بشكل استثنائي (المعهد الفرنسي للتحليل الاستراتيجي، 2012). يستمر المقال في التعريف بأسماء أكثر من 1500 قائد من قادة الحروب الإلكترونية في الباسيج. كما يشرح المقال أيضاً قوات شرطة الفضاء الإلكتروني الإيرانية التي تأسست من أجل الحفاظ على منهاج وصوت ولغة الثورة في مواقع الويب ومواقع التواصل الاجتماعي التي تستضيفها إيران على شبكة الإنترنت.

يدل التوسع الأكاديمي والتحول إلى عمليات في الفضاء الإلكتروني على التزام قومي بحماية البنية التحتية الحيوية وأيضاً تطوير طرق العمليات العدائية المضادة للعمليات العدائية الهجومية في الفضاء الإلكتروني التي تقوم بها إيران.

تُقدِّم جامعة الشريف دورات دراسية تقليدية في أمن المعلومات والتكنولوجيا وتوسعت في ذلك وانتقلت إلى مواضيع متقدمة. تغطي بعض الموضوعات التي تدرسها الجامعة:

- الأمن المتطور للشبكات CE 40-817
  - الجدران النارية، IDS/NIDS، DoS/DDoS، أمن التتبع، الأمن اللاسلكي، وأمن الويب
  - (أي ملفات تعريف الارتباط، والخداع الإلكتروني، الخ)، وتحليل الخصوصية/الحركة على الإنترنت، وإخفاء الهوية (استخدام حصان طروادة/(Tor))، وبرامج الديدان/البرامج الخبيثة الضارة، ومصائد مخترقي الشبكات (Honeypots)، وتحليلات الأدلة الجنائية على الشبكات، وأمن بروتوكول نقل الصوت عبر الإنترنت (VoIP) (خرازي، 2014)

عند إلقاء نظرة عن كثب على هذا الموضوع نكتشف الحاجة لوضع خط أساسي لفهم الأمن والخصوصية بالإضافة إلى تصنيف حيوي قياسي مع الهجوم الفوري على القراصنة وأعمال القرصنة. (خرازي، سي إي 817 أمن الشبكات المتطور صفحة 817 – 902، محاضرة 2012).

يغطي البروفيسور خرازي في محاضرته الثغرات والتهديدات ويعلق على ذلك بقوله "لا يمكنك وضع تصميم نظام أمني (خرازي سي إي 817، أمن الشبكات المتطور الصفحات 817 – 902 ما لم تعرف من هو عدوك" محاضرة، عام 2012)

تغطي المحاضرة القراصنة وجرائم القرصنة المنظمة وغير المنظمة، وأعمال التجسس، والأعمال الداخلية القذرة والجواسيس وأيضاً طرق الهجوم التقليدية مع الاعتراف باقتباس مواد مصدر البحث من جامعة كولومبيا وجامعة جورج واشنطن. في الواقع تشير كل محاضرة من المحاضرات إلى المصادر الغربية للمواد العلمية المثبتة والمعترف بها.

مثل معظم المحاضرات الجامعية من هذا النوع هذه المحاضرة مصحوبة بمعامل عملية. يغطي البروفيسور خرازي الأنشطة المعملية مثل اختراق المنافذ، وتقييم الأعمال اللاسلكية باستخدام WireShark والمصايد.

المصائد هي نوع من المصائد مفتوحة المصدر. حيث يتم تكليف الطلبة بمهمة إنشاء موقعي استضافة كاذبين على بيئة التشغيل Windows و Linux باستخدام Nmap و Hping في إجراء مسح على مواقع الاستضافة الافتراضية. يُطلب من الطلبة تتبع أنشطة

تسجيل الدخول ومقارنة النتائج مع مصايد العسل (خرازي سي إي 817، كراسة واجبات الأمن المتطور للشبكات 2، 2014). من خلال الإعدادات التي تم تقديمها نجد أن سوريا ليست على درجة عالية من التطور ولكنها تتعلم من حليفتيها روسيا وإيران. تمثل الجامعة السورية الافتراضية وجامعة تشرين نموذجين للبرامج الأكاديمية التي تسعى لفهم العمليات التي تتم في الفضاء الإلكتروني وتعليم وتثقيف القوى العاملة من أجل حماية البنية التحتية الحيوية السورية.

مهام القبض على العلم (Capture the Flag)

ترعى جامعة الشريف في الوقت الحالي وقائع مسابقات القبض على العلم Capture the Flag (CTF). تضمنت مسابقة عام 2014 القبض على العلم في مجالات تغطي هجمات الويب وعلم وفن كتابة الرسائل بطريقة خفية لا يمكن اكتشافها وعلم التشفير والأدلة الجنائية والأكواد الآمنة والهندسة العكسية والاستطلاع والاستكشاف (جامعة الشريف، 2014).

وتمت ترجمتها باستخدام مصطلحات طرق وأساليب ووسائل التجسس التقليدية، تدرب جامعة الشريف الطلاب من خلال عمليات عدائية في الفضاء الإلكتروني، واستخدام طريقة الخداع والإنكار وطرق وأساليب استقصائية وإجراءات وقائية ودفاعية في الفضاء الإلكتروني وجمع معلومات استخباراتية في الفضاء الإلكتروني. هذه المسابقة مسابقة دولية في طريقة تعاملها ويتم نشر جميع الأبحاث المكتوبة (نتائج أنشطة القبض على العلم CTF) ومراجعتها وتحليلها. هذه الأبحاث المكتوبة توفر مادة تعليمية للجميع بعد انتهاء أنشطة القبض على العلم CTF. تشمل أعلى 10 نتائج في مسابقة 2014 حوالي 1173 فريق:

جدول 1 نتائج جامعة الشريف في مسابقة القبض على العلم CTF لعام 2014

الترتيب	الفريق	الدولة	التصنيف
1	Dragon Sector	الصين	1467.569
2	Plaid Parliament of Pwning	الولايات المتحدة الأمريكية	1370.145

3	More Smoked Leet Chicken	روسيا	1027.791
4	StratumAuhuur	ألمانيا	815.703
5	penthackon	المملكة المتحدة	683.298
6	tomcr00se	الولايات المتحدة الأمريكية	650.838
7	int3pids	أسبانيا	587.065
8	Samurai	الولايات المتحدة الأمريكية	574.472
9	BalalaikaCr3w	روسيا	530.757
10	Eindbazen	هولندا	523.207

تدل درجات الفريق الإيراني (جدول 2 في الأسفل) على أنه ما زال أمامها طريق طويل تقطعه لكي تحقق درجات أعلى 10 فرق الموضحة في الجدول 1. إلا أن نفقات وحجم وحدة الحرب الإلكترونية في الفضاء الإلكتروني التي تصرف على قوات حرس الثورة الإسلامية والتي يصل عدد العاملين فيها إلى 2400 شخص بميزانية 76 مليون دولار أمريكي (جيمس أ لويس، 2011). توضح القدرات والإمكانيات الإيرانية بناءً على هجوم شامون على المملكة العربية السعودية زيادة في القدرات والإمكانيات مدفوعة بسياسة خارجية.

انتشر فيروس شامون عبر أجهزة الكمبيوتر وأجهزة الشبكات المشتركة وقام بمسح الأجهزة وسجلات التشغيل الرئيسية للأجهزة لمنعها من التشغيل. يقال أن هذا البرنامج قد استمد طرق عمله من البرامج الخبيثة السابقة التي بقيت في ميدان المعركة على الفضاء الإلكتروني بدون تشفير حمولة الهجوم.

جدول 2 نتائج الفريق الإيراني:

#	Team	Trivia	Crypto	Stegano	Forensic	Web	Reverse	Sec	Misc	bonus	Total
respina	1	125	0	340	0	150	340	500	400	0	1,855
arch	2	100	0	100	0	158	310	525	240	0	1,433
hithaegl	3	125	0	0	0	510	0	530	240	0	1,405
baghali	4	125	0	350	0	150	320	0	410	50	1,405
dalt0n	5	125	0	0	0	480	100	200	430	0	1,335
jolbakz	6	25	0	0	0	150	0	560	440	50	1,225
neridah	7	100	0	0	0	150	0	520	420	0	1,190
caspian	8	150	0	105	0	150	320	200	200	0	1,125
aaa	9	50	0	0	0	180	105	540	200	0	1,075
geek	10	75	0	100	0	150	200	0	440	0	965

نضج النموذج في كلٍ من سوريا وإيران للمرحلة التي كانت تعمل فيها مجموعات أشيان في جيش الفضاء الإلكتروني الإيراني، والجيش الإلكتروني السوري على إحباط رغبة الشباب المراهقين في التعزيز الصريح والواضح والذي من المفترض أن تكون نتيجته حكومة جديدة منتظرة تهيمن على الأوضاع. يستخدم العديد من المؤسسات الافتراضية الخارجية التي تحاكي الكيانات الفعلية كوكلاء في الفضاء الإلكتروني. تعد حماس وحزب الله نموذجين على الوكلاء الذين يوفرون الدعم الأساسي الملموس لإيران.

تستهدف مؤسسات في الفضاء الإلكتروني مثل كتائب الشهيد عز الدين القسام المصالح الإسرائيلية والغربية وتزعم أنها ضربة العديد من المواقع الإسرائيلية بمساعدة مجهولين في عام 2013 وتسببت في خسائر قيمتها 55.4 مليون دولار (كتائب الشهيد عز الدين القسام، 2013).

شملت مشاركة الجيش الإلكتروني السوري في هذا الهجوم تلقي تعليمات عبر البريد الإلكتروني من الأعضاء الذين يقومون بتوثيق استخدام الأدوات والأهداف (Treadstone 7، 2014).

القوة الإسرائيلية الضخمة في الفضاء الإلكتروني

وضعت الجامعات الإسرائيلية مثل جامعة تل أبيب ومعهد الدفاع الإسرائيلي في الفضاء الإلكتروني وجامعة بن جوريون منهجاً لأمن الفضاء الإلكتروني والاستخبارات. يركز منهج جامعة بن جوريون على الأمن التقليدي للفضاء الإلكتروني بالإضافة إلى دورات دراسية في علوم التشفير وأمن الشبكات وأمن نظم التشغيل واستكشاف الهجوم وهندسة نظم الأمن وتنمية الوعي الأمني.

معهد الدفاع الإسرائيلي في الفضاء الإلكتروني اسم على مسمى لأنهم يقومون بتدريس دورات في نظام التشغيل Linux والهندسة الأمنية والعمارة الأمنية وزيادة الأمان في برنامج التشغيل windows ومشاريع التطوير والحوكمة والإدارة والأمن. الدورة الوحيدة التي تحيد عن هذا المنهج هي دورة أساليب القرصنة.

تُدرس جامعة تل أبيب هذه المراجع إلا أنه لا يوجد دليل واضح وصريح على هذا المنهج وهذه البرامج. في الواقع لا يوجد شرح للعمليات الدفاعية الصريحة التي تتم على الفضاء الإلكتروني، وأعمال الاستخبارات التي تتم على الفضاء الإلكتروني / أو المناهج العدائية على الفضاء الإلكتروني ولا يمكن العثور على أي من ذلك في أي مكان.

ليس من المعتاد التشويش على هذه المعلومات كطريقة لحماية مواد الدورة الدراسية ومن ثم إمكانيات الطلبة حديثي التخرج.

كانت إسرائيل منذ أمد بعيد على رأس هرم أمن الفضاء الإلكتروني من خلال تأسيس مجتمع ناشئ متعطش لذلك. تجد العديد من الشركات الناشئة جذورها في قوات ومؤسسات الدفاع الإسرائيلية مثل مؤسسة 8200 (ثمانية آلاف ومئتان) التي تركز على الاستخبارات في الفضاء الإلكتروني وعمليات التجسس والتخريب.

تعد إسرائيل واحدة من المواقع الرائدة على مستوى العالم في مجال أمن الفضاء الإلكتروني بالتوازي مع وادي السليكون والعديد من مجالات ومناطق البحث الأخرى في الولايات المتحدة وفي أنشطة التطوير وإنشاء الشركات.

تركز الاستثمارات الضخمة من الولايات المتحدة على مراكز التفوق والامتياز في بير شيفا.

فقد استثمرت شركات مثل EMC و IBM و Lockheed Martin بقوة في رأس المال الإسرائيلي وقامت بتأسيس محور بير شيفا كمحور لأمن الفضاء الإلكتروني في إسرائيل. وقد جذب رئيس الوزراء استثمارات وبذل طاقة هائلة في تسويق هذا المجال من خلال المكتب القومي للفضاء الإلكتروني، وإطلاق CyberSpark ومسابقة الإبداع الإسرائيلي في مجال الفضاء الإلكتروني.

يعمل المكتب الوطني للفضاء الإلكتروني على تقديم المشورة لرئيس الوزراء في ثلاث مجالات رئيسية:

1. تطوير الدفاع وبناء قوة وطنية في مجال الفضاء الإلكتروني
2. تعزيز ريادة إسرائيل في مجال الفضاء الإلكتروني
3. تطوير العمليات التي تدعم أول مهمتين (المكتب الوطني للفضاء الإلكتروني، 2011)

نظرة عن كثب على القرار رقم 3611 توضح الالتزام بالدعم من طرف لآخر:

المادة 16) تطوير التنسيق والتعاون بين الهيئات الحكومية والجهات المسئولة عن الدفاع والهيئات الأكاديمية والهيئات الصناعية والشركات والهيئات الأخرى التي لها علاقة بمجال الفضاء الإلكتروني (المكتب الوطني للفضاء الإلكتروني، 2011).

توضح المادة 16 بجلاء المتطلبات اللازمة من أجل إنشاء منهج وطني كامل وشامل لأمن الفضاء الإلكتروني. كما هو الحال مع غالبية الوثائق الإسرائيلية من هذا النوع ليس هناك ذكر مباشر للعمليات الهجومية في الفضاء الإلكتروني.

ومع هذا هناك بعض الدلائل على أن الوحدة 8200 تركز على الإشارات الخاصة بالاستخبارات؛ والوحدة 504 تركز على العامل البشري في الاستخبارات والاستقصاء؛ كما تركز الوحدة 5114 على عمليات المراقبة والمسح باستخدام الراديو؛ كما تركز الوحدة هاتزفار على الاستخبارات مفتوحة المصدر وعلى اللغة (الأمن الدولي، 2011)، كما تركز الوحدة باهاد 15 على حرفية الاستخبارات (Wikimapia, n.d.)، كما تستهدف وحدة أمن المعلومات IDF أمن نظم الحاسوب وأمن الوثائق السرية.

عمليات الفضاء الإلكتروني على أرض الواقع

لقد كان هناك تيار متواصل من هجمات الفضاء الإلكتروني التي يتم تنفيذها في الشرق الأوسط خلال السنوات القليلة الماضية. فيما يلي قائمة ووصف لهذه الهجمات بناءً على الدول الثلاث التي نغطيها في هذا الفصل وذلك بناءً على البيانات التي تم جمعها من Hackmageddon (www.hackmageddon.com).

قام الجيش السوري الإلكتروني بالقرصنة على الموقع الرئيسي لجامعة هارفارد في 26 سبتمبر 2011 تاركاً على واجهة الموقع رسالة تدل على أنه كان هناك. في 17 يناير 2012 وقع هجوم يعزى لفريق IDF بأنه قام بتعطيل موقعي البورصة في كل من السعودية ودولة الإمارات العربية المتحدة.

من المفترض أن IDF يقف في مواجهة قوات الدفاع الإسرائيلية لكن هذا غير مؤكد. في 20 يناير من نفس العام أعلنت مجموعة القرصنة الإسرائيلية TheJ0k3rS أنها قامت بالسيطرة على العديد من مواقع الويب الإيرانية وأعلنت عن شريط فيديو يوضح الهجوم والقرصنة.

في حركة دفاعية تستهدف التدريب عقد مكتب الإدارة الوطنية للفضاء الإلكتروني الإسرائيلي أول مهمة إرهاب له في الفضاء الإلكتروني وأطلق عليها "إطفاء الأنوار" وتحاكي الهجمات على البنية التحتية المهمة في 25 يناير 2012.

كأحد المهام المحتملة في هذا التدريب تسيطر وحدة IDF على العديد من المواقع الحكومية والإعلامية الإيرانية وتنشر عليها علم إسرائيل في 26 يناير.

استجابة لتركيز جامعة تل أبيب على أمن الفضاء الإلكتروني من قبل هيئة الدفاع الوطني عن الفضاء الإلكتروني، يخترق قراصنة مجهولين من الشرق الأوسط الموقع ويتركون صوراً لحرق العلم الأمريكي والعلم الإسرائيلي. وعلى الرغم من اعتبار هذا النوع من الهجوم نوعاً من التشويه إلا أن حرج الإسرائيليين السياسي منه كان كبيراً. وفي فبراير 2012 أعلنت بعض الجهات من إيران مسئوليتها عن الهجوم.

في 13 فبراير أعلنت إيران أن منشآتها النووية محصنة من هجمات الفضاء الإلكتروني في ضوء الهجمات السابقة من Stuxnet و Duqu مع إعلان القائد الأعلى للثورة الإيرانية السيد علي خامنئي عن تشكيل مجلس أعلى للفضاء الإلكتروني (7 مارس).

ثم عقدت إيران أول مؤتمر حول أمن الفضاء الإلكتروني وقد كان السيد بهروز كامالیان من مجموعة آشیان الأمنية الرقمية المتحدث الرئيسي في هذا المؤتمر.

ومع استعراض عضلاته الجديدة في الفضاء الإلكتروني يهاجم الجيش الإلكتروني الإيراني دولة أذربيجان وهي دولة حليفة لدولة إسرائيل ويترك رسالة عن كونها خادمة لليهود.

أعقب هذا الهجوم هجوم من الحليف الإيراني جيش حزب الله للفضاء الإلكتروني على موقعين لاثنين من المصلحين الإيرانيين المناهضين للحكومة.

أهم هجوم في 2012 مرتبط بالدول المستهدفة هو هجوم شامون في 15 أغسطس. تعرض موقع شركة أرامكو السعودية للضرب من قبل فيروس يكرر نفسه انتشر على أكثر من 30000 جهاز يعمل بنظام النوافذ (Windows) وقام بمحو الأقراص الصلبة وسجلات

بدء التشغيل الرئيسية للأجهزة وقام بتعطيلها. تعقيد هذا البرنامج الخبيث الضار وضع إيران على الخريطة كقوة في مجال الحرب الإلكترونية التي لا طائل من ورائها (أكوهيدو، 2013).

ومع بداية عام 2013، بدأت إيران في إظهار مخالبها في مجال التجسس والتخريب الإلكتروني. حيث وقعت سلسلة من الهجمات ضد البنوك الرئيسية الكبرى في الولايات المتحدة في صورة تكرار رفض الخدمة واستخدم في هذا الهجوم مراكز بيانات من جميع أنحاء العالم مصابة ببرنامج خبيث يعرف باسم 'itsoknoproblembro' تم تصميمه من أجل تعطيل عمل مضادات الفيروسات (بيترسون، 2013). يذكر أن إيران قامت بقرصنة أجهزة الكمبيوتر غير المصنفة في البحرية الأمريكية في محاولة للتجسس في الفضاء الإلكتروني في سبتمبر 2013.

تمكن SEA من صد هجوم قرصنة شديد القوة على حساب وكالة أسوشيتد برس للأخبار على موقع تويتر وقام بنشر تقرير إخباري كاذب عن انفجار وقع في البيت الأبيض تسبب في انخفاض قصير الأجل في أسعار أسهم البورصة الأمريكية. في 2 سبتمبر 2013 قام SEA بالقرصنة مرة أخرى على موقع البحرية الأمريكية في تدريب من أجل تشويه ذكرى سيناريو الأنشطة البدائية. شهد عام 2014 قرصنة SEA على مدونة ISD الرسمية أعقبها قرصنة على حساب الجيش الإسرائيلي على موقع تويتر يحذر من تسريب نووي في مفاعل ديمونة.

تنامي النضج

دلت سلسلة هجمات القرصنة على تنامي نضج إمكانيات القرصنة واستخدام أحمال المواقع المستهدفة. من الواضح من خلال هذه النوعية من الهجمات ومن الطرق المستخدمة فيها أن إيران قد تطورت تطوراً كبيراً يتجاوز قدرات SEA على التكييف مع نفس المنهج الشامل مثل الإسرائيليين. يكفي أن نقول أن السوريين قد سيطروا مبكراً على ميدان المعركة الداخلية. فقد كان الهدف خلال هذه المراحل المبكرة من الحرب الإلكترونية هو:

- القيام "بضربة مؤثرة" ضد العدو المتوقع
- إحراج الموقع المستهدف من خلال إظهار المشاكل الأمنية
- جذب انتباه العامة لقضية ما أو "اضطهاد" أو كيان ما

- تحدي / رفض استخدام خادم موقع الويب غير الرسمي من قِبل أحد المؤسسات
- خفض ثقة عامة الناس في أمن أحد النظم ومدى جدارته للاستخدام في أغراض حساسة
- إجبار النظام المستهدف على الخروج من الخدمة إلى حين إمكانية تأمينه / تحليله، وتنسيقه من جديد وإعادة بناؤه وتقويته
- تأسيس "مصداقية لدى رجل الشارع" مع أقران القراصنة / المخترقين أو فقط بمجرد أن من يقوم بالتشويه يجد في التشويه "متعة"

بصرف النظر عن الهدف فإن المهارات والخبرات التي يتم اكتسابها خلال هذه المسابقات تعمل على زيادة المجموعات المشاركة وزيادة الجرأة لديها.

أسلحة الفضاء الإلكتروني

هناك العديد من أنواع الأسلحة المستخدمة في حروب الفضاء الإلكتروني. فقد شهد العالم أسلحة تشبه Stuxnet و Duqu وأيضاً Flame و Shamoon. وقد قادت الأسلحة التي ما زالت مستخدمة في ميدان معارك الفضاء الإلكتروني إلى تعديلات وتطورات مبتكرة. وقد أدت الأسلحة ذات الأحمال غير المشفرة إلى الهندسة العكسية للأحمال كسلاح فعلي يتم الاستيلاء أو الاستحواذ عليه خلال العمليات الحربية ما أدى إلى اكتشاف الأعداء لتقنيات فريدة من نوعها. في عام 2003 ذكر تقرير حول استبيان عن (الأسلحة صغيرة الحجم) أن 1134 شركة على الأقل في 98 دولة على مستوى العالم شاركت في بعض جوانب إنتاج أسلحة و/أو ذخائر صغيرة الحجم.

كما أن الصادرات الضخمة للولايات المتحدة والاتحاد السوفيتي السابق والصين وألمانيا وبلجيكا والبرازيل من الأسلحة صغيرة الحجم أثناء الحرب الباردة كانت على نطاقٍ تجاري من أجل دعم الحركات الإيديولوجية. وقد حافظت هذه الأسلحة صغيرة الحجم على مكانتها خلال العديد من النزاعات وأصبح العديد منها حالياً في متناول تجار الأسلحة أو الحكومات الصغيرة التي تقوم بتحريك هذه الأسلحة بين مناطق النزاعات حسب الحاجة.

تدل الأنشطة السابقة لمجموعة أنونيموس (Anonymous) على انتشار نفس نوعية الأسلحة صغيرة الحجم في الخطط والطائرات الافتراضية.

مدفوعة إلى حد كبير بأنشطة أيديولوجية، وقد قامت منظمة أنونيموس (Anonymous) بتوزيع إصدار متجدد من الأداة Low Orbit Ion Cannon (LOIC) المستخدمة على نطاق واسع في هجمات رفض توزيع الخدمة (DDoS).

وقد كانت أداة LOIC هي السلاح الرئيسي الذي استخدمته منظمة أنونيموس في "عملياتها العدائية المستمرة" وحملات DDoS ضد مؤسسات صناعة الأفلام والتسجيلات، وأيضاً مؤسسات أخرى متورطة في أنشطة مناهضة للتجسس. هذا التطبيق أنشأه في الأساس مستخدم يعرف باسم Praetox وقد تم استخدامه في العديد من الهجمات الشاملة على مدار سنوات بما في ذلك حملات منظمة أنونيموس ضد الكنيسة العلموية (Church of Scientology) أو الحكومة الاسترالية أو مظاهرات الانتخابات الإيرانية العام الماضي.

في يناير 2009 تم إطلاق شفرة برنامج التشغيل Windows على Source Forge كمشروع مفتوح المصدر وتم إنشاء إصدار من برنامج Java متعدد المنصات بعد ذلك بفترة. هذا الإصدار يتيح نشر الكود الذي يمكن تطويره وتحديثه واستخدامه في النزاعات منخفضة الحدة مع احتمال تغطيته بصورة كبيرة من قبل وسائل الإعلام.

في العام الماضي قام مطور آخر باختراق الشفرة وأضاف ميزة جديدة تعرف باسم "Hive Mind" للأداة. تتيح هذه الميزة للمستخدمين بمنع السيطرة على التطبيق بعد عملية التثبيت وجعله يتصرف كعميل botnet، والذي يمكن التحكم فيه من خلال قناة IRC. هذه الطريقة لنشر الأسلحة الافتراضية صغيرة الحجم تتيح للأفراد الذين لهم نفس الأفكار والعقلية الذهنية المشاركة في أنشطة DDoS بناءً على أيديولوجيتهم مع منح السيطرة للمصادر المركزية. حجب منظمة أنونيموس من قبل حكومات دول الشرق الأوسط يرجح إمكانية التأثير وتوجيه هجمات مباشرة ضد الأعداء الذين يعملون كوكلاء جهلاء يستخدمون كأداة في السياسة الخارجية.

الأسلحة صغيرة الحجم والأسلحة الخفيفة مسئولة عن غالبية حالات وفيات المعارك في الحروب المعاصرة ولها دور في الكثير من الجرائم والعنف المدني الذي تتعرض له المجتمعات الهشة في جميع أنحاء العالم (كلار).

الأسلحة صغيرة الحجم مسئولة في الوقت الحالي عن جميع الأنشطة الضارة حول العالم حالياً.

وسوف يستمر ذلك في المستقبل القريب كما سيكون آفة معظم الحكومات وأي شخص لا يتفق مع إحدى المجموعات التي لديها القدرة على القيام بالثأر فعلياً في العالم الافتراضي ورصد ومراقبة ومنع حق الاعتراض أو أن يكون للشخص أيديولوجية مختلفة. الأسلحة الافتراضية صغيرة الحجم تعمل أيضاً كأرضية تدريب لدول مثل سوريا وإيران.

الأسلحة الافتراضية صغيرة الحجم طرق مثالية لإحداث اضطرابات على الإنترنت. لأنها متاحة على نطاق واسع ومنخفضة التكاليف هذا لو كانت لها تكلفة بالفعل على الإطلاق، لأنها تمثل ضغط هائل وسهلة الاستخدام وسهلة الحمل وسهلة التعامل معها، وربما تكون لها استخدامات شرعية عسكرية أو شرطية أو مدنية (كلار). هذه الأسلحة الافتراضية خفيفة الأثر ويمكن استخدامها من قبل الشباب الغض صغير السن جداً الذين يفتقرون الخبرة الفنية ولعبوا دوراً كبيراً في النزاعات الافتراضية مؤخراً.

لكن وبمجرد انتهاء أحد النزاعات الافتراضية، فما زالت الأسلحة صغيرة الحجم موجودة في أيدي المشاركين، يمكن استخدام الأسلحة الافتراضية صغيرة الحجم بسهولة في بدء النزاعات التي قد يكون لها طابع شخصي كبير. لأنها تخلق فائضاً من الأسلحة الافتراضية صغيرة الحجم وتؤسس لثقافة القرصنة ودائرة لا تنتهي من النزاعات الافتراضية. وقد استفادت منظمة أشيان و SEA والجيش الإلكتروني الإيراني من النزاعات الافتراضية لمنظمات الاختراق الأخرى مثل منظمة أنونيموس في تعلم تكتيكات وأساليب وبروتوكولات جديدة. وقد استفادت هذه المجموعات أيضاً من خلال الاستحواذ على الأسلحة الافتراضية صغيرة الحجم من ميدان الحرب الإلكترونية في الفضاء الإلكتروني.

كان هناك قلق في الماضي من أن منظمة أنونيموس قد استحوذت على الكثير من الأكواد المرتبطة ببرنامج Stuxnet وضمنت استحواذ الدول على الكود أيضاً. طبقاً لبعض "الخبراء" فإن هذا البرنامج الخبيث يعتبر إلى حد كبير حدوداً مجهولة لمنظمة أنونيموس، "والتي بنت سمعتها على اختراق مواقع الحكومات والشركات متعددة الجنسيات على الإنترنت، مثل شركتي Visa و MasterCard وهو ما يعتبر تهديداً لحرية التعبير (هاليداي، 2011)."

المشكلة هي أنه لا أحد بالفعل يعرف إمكانيات وقدرات منظمة أنونيموس التي هي عبارة عن شبكة مفككة تجمعوا معاً للنيل من الأهداف الجماعية والقيام بهجمات بناءً على أيديولوجية مشتركة أو معتقد مشترك. تستخدم منظمة أنونيموس تقنيات الجيل الثاني من الويب Web 2.0 لتأسيس تصميم مجتمعي لجهودهم المركزة. كما أنهم يستخدمون تقنيات الجيل الثاني من الويب للارتقاء بمجهوداتهم لمستويات جديدة.

الطرق التي تستخدمها منظمة أنونيموس تمثل حجرات دراسة افتراضية للمؤسسات السورية والإيرانية الحكومية وغير الحكومية. الأسلحة الافتراضية صغيرة الحجم المتبقية التي تركتها Stuxnet والأسلحة الافتراضية صغيرة الحجم الأخرى توفر قاعدة من أجل القيام بهجمات جديدة يمكن الارتقاء بها إلى حدٍ بعيد بنفس طريقة الارتقاء بسلاح LOIC ونضجه بمرور الزمن.

الطرق التي لا رابط بينها للقيام بعمليات قرصنة تقوم بها منظمة أنونيموس تمثل مدى لإطلاق نيران الحرب في الفضاء الإلكتروني وتعمل كأرضية اختبار وإثبات لكفاءة الأسلحة.

توفر لنا قائمة أسلحة الحرب الإلكترونية الحالية رؤية ومنظوراً حول تنامي تعقيدات ومدى فداحة الهجمات. لأن التطفل والتصيد قد يعملان معاً على توفير اختراق أولي للأهداف. بمجرد استطلاع الأهداف يتم تنزيل أحمال جديدة على الموقع المستهدف تم تصميمها خصيصاً للموقع المستهدف بناءً على معلومات استخباراتية تم جمعها لهذا الغرض. قد تكون الأحمال الجديدة ما هي إلا أساليب لتطوير الاستخبارات في الفضاء الإلكتروني. قد تتضمن الأحمال طرق استخبارات وتخريب.

قد تستهدف الأحمال نظم تشغيل وأجهزة معينة. يمكن أن تعمل الأحمال كأداة أولية في جمع البيانات متضمنة داخل برنامج خامل يتم تنشيطه في حالة النشاط الفعلي أو حروب الفضاء الإلكتروني. قد تكون الأحمال قاتلة من منظور حركي لأنه ينتج عنها حصيلة فعلية نتيجة النشاط على الفضاء الإلكتروني. قد يكون للأحمال أيضاً أثر غير قاتل أو ضار أو حركي نتيجة رفض دخول الأعداء على أسلحة الحرب الإلكترونية الخاصة بهم.

هاجمت أسلحة الفضاء الإلكتروني أسماء نطاقات النظم وبوابات البروتوكولات وبروتوكولات الإنترنت الأساسية. وقد استخدمت Botnets في تنفيذ عمليات هجوم لتكرار رفض الدخول على الخدمة. وتم استهداف نظام SCADA وأيضاً البنية التحتية الحيوية الأخرى. يوضح أحد الاختبارات على أنشطة القبض على العلم (CTF) في إيران استخدام هذه الأسلحة أثناء ألعاب وحروب القبض على العلم.

موقف الولايات المتحدة واستعداداتها

الولايات المتحدة في موقف جيد كواحد ممن يملكون قدرات حروب الفضاء الإلكتروني إن لم تكن الرائدة في هذا المجال. توضح تعديلات العام المالي 2013 على ميزانية الكونجرس للاستخبارات الوطنية خمس مبادئ رئيسية إرشادية تمت صياغتها في جميع بنود الميزانية:

- احتفاظ الولايات المتحدة بقوة عمل ماهرة ومدربة؛
- تركيز الولايات المتحدة بشكل أكبر على التكامل والتعاون؛
- دعم ومساندة الإمكانيات الذكية التي تدعم العديد من المهام؛
- تطوير الاستخبارات المعادية؛ و

- حماية الاستثمارات الرئيسية للمستقبل (برنامج الاستخبارات الوطني، 2012).

على الرغم من وجود بعض الاستقطاعات والتوفير المحدود داخل الميزانية فإن المجالات الرئيسية المستمرة في النمو تمثل مجالات داخل نطاق دورة حياة الاستخبارات في الفضاء الإلكتروني، وأمن الفضاء الإلكتروني والاستخبارات المعادية والعلوم والتقنيات التي تركز على مهام محددة وجميع التقنيات التي لها مكونات تدخل في الفضاء الإلكتروني. تتطلب الميزانية إظهار التزام محدد بقدرات وإمكانيات الحرب في الفضاء الإلكتروني.

الأمر الرئاسي رقم 20 والمتعلق بالتوجهات السياسية (PPD20) يحدد للحكومة الأمريكية توجهها في تطوير وتنمية قدرات الحرب الإلكترونية والحفاظ عليها. يحدد القرار الرئاسي PPD20 بوضوح العمليات الهجومية الفاعلة في الفضاء الإلكتروني، وعمليات الفضاء الإلكتروني التي لها عواقب خطيرة والتعامل مع الأنشطة الخبيثة المستمرة في الفضاء الإلكتروني كمجالات ومناطق تنمية (البيت الأبيض، 2013).

تركز قدرات العمليات الفاعلة في الفضاء الإلكتروني على عمليات الفضاء الإلكتروني ضد الأعداء والتي قد تسبب أضرار تتراوح من خفيفة إلى ضارة (البيت الأبيض، 2013). عمليات الفضاء الإلكتروني التي لها عواقب خطيرة تتطلب موافقة رئاسية بينما الاستجابة للأنشطة الخبيثة المتواصلة على الفضاء الإلكتروني يقصد بها الهجمات المعادية التي تهدف إلى تخفيف أثر الهجوم وعقاب الجهة المهاجمة بناءً على ضعف كفاءة دفاع الشبكة أو تفعيل القانون (البيت الأبيض، 2013). يستدعي كل من القرار الرئاسي PPD20 وتعديل الميزانية الخاصة بالاستخبارات الوطنية بتطوير مشاركة البيانات عبر المؤسسات الفيدرالية والمؤسسات الشريكة، وهذا أحد الجوانب المهمة الناجحة والمتكاملة لحروب الفضاء الإلكتروني.

يجب على الولايات المتحدة الاستمرار في تطوير القوى العاملة ذات التعليم الجيد من خلال التعاون مع المجتمع الأكاديمي. تنفيذ العديد من البرامج الخاصة بأمن الفضاء الإلكتروني وعمليات الفضاء الإلكتروني واستخبارات الفضاء الإلكتروني وزيادتها على مستوى الطلبة ومستوى الخريجين. وجود برامج تدريب تجارية لتدريب مقاتلي حروب الفضاء الإلكتروني وأخصائيي تجميع البرامج مفتوحة المصدر. برامج دورات التدريب الخاصة باستخبارات الفضاء الإلكتروني متاحة للحكومة والهيئات العسكرية والتجارية.

قد لا تدعي هذه البرامج والدورات التدريبية بشكل صريح أنها برامج مخصصة للهجمات على الفضاء الإلكتروني كجزء من المنهج الدراسي إلا أن هذه الدورات تُعلم أساليب الإنكار والخداع والهدم والتخريب والاختراق والتلاعب وأيضاً القدرة على تدمير أنظمة الكمبيوتر والمعلومات. هذا البرنامج المختلط يضمن قوى عاملة مدربة.

مدى أنشطة القبض على العلم وحروب الفضاء الإلكتروني يضمن إجراء اختبارات شاملة على الأسلحة ووجود برامج تدريب على الأسلحة والعمل على توفير "مخزون قطع غيار" للبرامج والأجهزة المستخدمة. قدرات وإمكانيات حروب الفضاء الإلكتروني في حاجة إلى عملية تسليح شاملة قبل إمكانية المصادقة عليها كنظم أسلحة حرب إلكترونية.

تمويل الولايات المتحدة لحروب الفضاء الإلكتروني يدل على التزامها بالتسليح من أجل الفضاء الإلكتروني. الاختلاف عن التسليح الفعلي هو أن أسلحة الفضاء الإلكتروني قد يكون لها فترة عمر قصيرة في المخزون نظراً لسرعة تغير بيئة الفضاء الإلكتروني. وهذا يتطلب اشتراطات متغيرة للتطوير باستمرار على عكس دورات الحياة الفعلية في السابق التي قد تستغرق سنوات لتطوير ونشر الأسلحة. وقد ينظر أيضاً لمقاتلي حروب الفضاء الإلكتروني على أنهم جزء من عملية التسليح لأن الضغط على أزرار لوحة المفاتيح بدون أسلحة قد يعمل على اختراق وتدمير وتخريب وإتلاف النظام المستهدف. يمكن تسليح مقاتلي الحروب الإلكترونية فقط من خلال التدريب والتعليم والمهارات العملية.

ينبغي أن يكون لدى نظام أسلحة حرب الفضاء الإلكتروني للولايات المتحدة إمكانية إصدار الأوامر والسيطرة على واختبار وسائل حماية محددة وطرق توصيل وأفراد مدربين وتكتيكات وأساليب وبروتوكولات ومحددات هجومية مختلفة ومنصات إطلاق (القيادة الإستراتيجية للولايات المتحدة، 2009).

الملخص

انتشار الإنترنت وانتشار قدرات أسلحة الفضاء الإلكتروني وتنسيق الجهود من أجل تدريب وتثقيف القوة العاملة كل هذه عوامل تسهم في سباق التسليح الحالي على الفضاء الإلكتروني. سواء كانت هذه الدولة هي سوريا أو إيران أو دولة إسرائيل فلا بد من التخطيط على المدى البعيد بأهداف وغايات واضحة من أجل تطوير ونشر ودمج قدرات حروب الفضاء الإلكتروني بشكل كامل.

أعداء الولايات المتحدة يؤسسون وبشكل سريع البنية التحتية اللازمة من أجل زيادة قدراتهم المعلوماتية وأظهروا براعتهم في ذلك.

يجب على الولايات المتحدة إنشاء برنامج شامل لحروب الفضاء الإلكتروني من أجل ضمان دمجه وتشغيله بالوظائف المتاحة حسب الطلب مع إمكانية الدخول عليه من جميع أنحاء العالم.

يجب على الولايات المتحدة الاستمرار في تطوير القوة العاملة ذات التدريب الجيد المصرح لها بالدخول على الأدوات والمنشآت اللازمة لتنفيذ أهداف السياسة الخارجية. مع القدرة على جمع البيانات وترتيبها وتنظيمها وإنتاجها مع تحليلها وتحويلها إلى إجراءات يمكن تنفيذها وتطبيقها على المستويين الاجتماعي والثقافي، وينبغي اعتبارها كعامل رئيسي في مجال الحرب الإلكترونية. وظيفة الاستخبارات هي وضع أسس الخطوات والإجراءات المستقبلية.

أعداء الولايات المتحدة في الشرق الأوسط كثيرين ويتعلمون استخدام الطرق وحقوق الملكية الفكرية الخاصة بالولايات المتحدة. من خلال سيناريو التجارب البدائية وأنشطة القراصنة النشطاء إلى مهام القبض على العلم CTF والبرامج التي ترعاها الحكومة، يزداد نضج عمليات الفضاء الإلكتروني بمعدلات سريعة. برامج الولايات المتحدة في حاجة لأن تكون دقيقة وقائمة على أساس التغير والتطور السريع وإمكانية التكيف من أجل الحفاظ على معدل السرعة والبقاء على قمة التكنولوجيا. يجب أن تكون البرامج إلزاماً قومياً مع خلق برامج تعليمية تعمل على إثراء العملية التعليمية التي تدير الفصول الدراسية داخل المدارس وحتى الدراسات الجامعية بالتوازي مع برامج فيدرالية، وثقافة مدرسية ولغوية، ودينية ومناهج تعليمية تقنية وفنية من أجل رفع كفاءة استهداف الأعداء في الشرق الأوسط. هذا النوع من المناهج يمكننا من فهم الخصوم المعروفين وليس فقط مجرد المادة المعرفية والخبرة العملية فقط. يجب أن يتسع نطاق مشاركة المعلومات ليتجاوز الكيانات الفيدرالية إلى المؤسسات الخاصة مع الخبرات والمهارات من أجل إتباع أهداف سياسة خارجية في حدود وقواعد المشاركة.

الولايات المتحدة في موقف ومنزلة جيدين يمكناها من تنفيذ هذه الإجراءات الإلزامية. لأن القيام بذلك يضمن القدرة على الاستجابة ورد الفعل السريع بكفاءة على تهديدات الفضاء الإلكتروني الحالية والمتوقعة من الشرق الأوسط.

الفهرس

Acohido, B. (2013, May 16). *Why the Shamoon virus looms as a destructive threat*. Retrieved from USA Today: http://www.usatoday.com/story/cybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/

American Intelligence. (2007, February 7). *Iran Launches Massive Exercise*. Retrieved from Amerian Inteligence: http://americanintelligence.us/iran-launches-massive-exercise/

Ashiyane. (2014, October 1). *Ashiyane*. Retrieved from Ashiyane Security Forum: ashiyane.org

Carroll, W. (2008, September 23). *Iranian Cyber Warfare Threat Assessment*. Retrieved from Defense Technology: http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment/

Cordesman, A. (2007, August 16). *Iran's Revolutionary Guards, the Al Qudes Force and Other.* Retrieved from Center for Strategic and International Studies: http://csis.org/files/media/csis/pubs/070816_cordesman_report.pdf

Defense Technology. (2011, February 28). *Defense Technology*. Retrieved from Social Networking Sites - Weapon, Threat and Target: http://defensetech.org/2011/02/28/social-networking-sites-weapon-threat-target/

Ezzedeen AL-Qassam Brigades . (2013, June 26). *Cyber attacks cause Israeli companies heavy losses*. Retrieved from AL-Qassam: http://www.qassam.ps/news-7167-Cyber_attacks_cause_Israeli_companies_heavy_losses.html

Global Security. (2011, September 7). *Israel IDF Military*. Retrieved from GlobalSecurity: http://www.globalsecurity.org/military/world/israel/general-staff.htm

Institut Francais d'Analyse Strategique. (2012, December 13). *Structe of Iran's Cyber Warfare*. Retrieved from Institut Francais d'Analyse Strategique: http://www.strato-analyse.org/fr/spip.php?article223

James A. Lewis, K. T. (2011). *Cybersecurity and Cyberwarfare.* Washington: Center for Strategic and International Studies.

Kharrazi, M. (2012, February 8). CE 817 Advanced Network Security 817-902 Lecture. Tehran, Iran.

Kharrazi, M. (2014, September 5). Advanced Network Security CE 40-817. Tehran, Iran.

Kharrazi, M. (2014, March 30). CE 817: Advanced Network Security Homework 2. Tehran, Iran.

Maslen, G. (2013, November 13). *Open Doors - Foreign Students Flock to America*. Retrieved from University World News: http://www.universityworldnews.com/article.php?story=20131114055159659

Muncaster, P. (2014, September 4). *Second Pro-Government Hacking Group 'Syrian Malware Team' Uncovered.* Retrieved from InfoSecurity Magazine: http://www.infosecurity-magazine.com/news/government-hacking-syrian-malware/

National Cyber Bureau. (2011, August 7). *Advancing National Cyberspace Capabilities.* Retrieved from National Cyber Bureau: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf

National Cyber Bureau. (2011, August 7). *Mission of the Bureau.* Retrieved from Mission of the Bureau: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx

National Intelligence Program. (2012). *FY 2013 Congresssional Budget Justification Volume I National Intelligence Program Summary*. Washington, DC: National Intelligence.

Peterson, A. (2013, January 9). *How Iranian Hackers Used the Cloud to Attack Major Banks and Why It Matters*. Retrieved from ThinkProgress: http://thinkprogress.org/security/2013/01/09/1424171/bank-hackings-iran-botnets-cloud/

Sharif University. (2014, September 29). *Fifth Annual Intrusion and Defend Competition in Cyberspace*. Retrieved from CERT Sharif University: https://cert.sharif.edu/?a=contentNews.id&id=128 and https://cert.sharif.edu/ctf

Smith, J. P. (2006, July 20). *DEVELOPING A RELIABLE METHODOLOGY FOR COMPUTER NETWORK OPERATIONS THREAT OF IRAN.* Retrieved from Federation of American Scientists: http://fas.org/irp/eprint/cno-iran.pdf

The programming unit in the Syrian Electronic Army. (2014, October 1). *SEA*. Retrieved from Syrian Electronic Army: http://sea.sy/index/en

The Whitehouse. (2013). *Presidential Policy Directive 20.* Washington, DC: US Government.

Treadstone 7. (2014, September 2). *Syrian Electronic Army Exposure Post 2 - Op Israel*. Retrieved from The Cyber Shafarat: http://cybershafarat.com/2014/09/02/syrian-electronic-army-exposure-post-2-op-israel-june-1-2013-uncovered-turkish-alignment/

USSTRATCOM. (2009). *The Cyber Warfare Lexicon.* Unknown: USSTRATCOM.

Wikimapia. (n.d.). *School for Military Reconnaissance (Bahad 15)*. Retrieved from wikimapia: http://wikimapia.org/26604922/School-for-Military-Reconnaissance-Bahad-15