أثر الإرهابي السيبراني على الأمن القومي

عميد دكتور / جلال فضل محمد العودي

أثر الإرهابي السيبراني على الأمن القومي

عميد دكتور / جلال فضل محمد العودي

إهداء

أهدي هذا البحث الذي يحمل عنوان (الإرهاب السيراني وأثره على الأمن القومي) لإخواني وزملائي الدفعة (٢٨) كلية الشرطة، وعميد الدفعة طارق محمد عبد الله صالح عضو مجلس القيادة الرئاسي

. . .

مقدمة

في ظل ثورة تكنولوجيا المعلومات سارعت مختلِف الجماعات الإرهابية والمتطرفة إلى إمتلاك مواقع على (الإنترنت)، وبخاصة شبكات التواصل الإجتماعي، وبعضها يمتلك أكثر من موقع وبأكثر من لغة، من أجل التعريف بالتنظيم وتاريخه ومؤسسيه وأنشطته، وخلفياته السياسية والإجتماعية، وأهدافه الفكرية والسياسية، وأحدث الأخبار، ومهاجمة خصومه من المفكرين والعلماء، ومن الحكومات والأجهزة الأمنية.

ففي عام ١٩٩٨ كان عدد المواقع الإرهابية على الشبكة العالمية للمعلومات أقل من ٢٠ موقعاً بينما تعد اليوم بالآلاف هذا عدا عن عشرات آلاف الصفحات الموجودة على الشبكات الإجتماعية، وأظهر تقرير حول النشاطات الإرهابية السيبرانية وقائع مقلقة إذ إستفاد الإرهابيون من نظم المعلومات والإتصالات العالية التقنية ما وفر لهم وسائل إتصال أمنة وسهلة وغير مكلفة على إمتداد العالم جعلت من الصعوبة بمكان مراقبتهم والحد من نشاطهم.

على سبيل المثال في السنوات الأخيرة، تمكن تنظيم داعش دعم قدراته الإلكترونية بدمج أذرعه (السيبرانية) مثل: "الخلافة الشبح" Ghost Caliphate، و"جيش أبناء الخلافة" Sons Caliphate Army، و"جيش الخلافة السيبراني" The Caliphate Cyber Army، و"كلاشينكوف الأمن الإلكتروني" Kalashnikov E-Security فيما سُمي (مجموعة قراصنة الخلافة السيبرانية المتحدة) The United

.Cyber Caliphate Hacker Group

وتمكنت مجموعة من القراصنة التابعين لتنظيم داعش في من إختراق بعض مواقع الشبِكة لتشويهها، ونشر الدعاية المتطرفة، مثل مواقع وزارة الصحة البريطانية، والشرطة الماليزية الملكية، والخطوط الجوية الماليزية، وشبكة التلفزة الفرنسية **TV5** والمحطات التابعة لها، والقيادة المركزية العسكرية الأمريكية.

وعليه سوف نقسم هذا البحث إلى المطالب التالية:

١- المطلب الأول: مفهوم الإرهاب السيبراني.

٢- المطلب الثاني: مفهوم الأمن القومي.

٣- المطلب الثالث: أثر الإرهاب السيبراني على الأمن القومي.

المطلب الأول

مفهوم الأمن السيبراني

أول ظهور لمفهوم الإرهاب الإلكتروني Cyber terrorism كان في ثمانينيات القرن العشرين، عندما عرفه باري كولين (Barry Collin) بأنه "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها, سعيًا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب".

ولكن لم يظهر الإرهاب الإلكتروني بصفة رسمية، إلا عندما قام الرئيس الأمريكي بيل كلينتون في عام ١٩٩٦ م بتشكيل هيئة حماية منشآت البنية التحتية الحساسة، وكان أول إستنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والإتصالات إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة، وبما أن هذه المنشأت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة، وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة، بإنشاء هيئاتها ومراكزها الخاصة، للتعامل مع إحتمالات الإرهاب الإلكتروني، فقامت وكالة الإستخبارات المركزية بإنشاء مركز حروب المعلوماتية، ووظفت ألفا من خبراء أمن المعلومات، وقوة ضاربة على مدى٢٤ ساعة لمواجهة الإرهاب الإلكتروني. وقامت القوات الجوية الأمريكية بإتخاذ خطوات مماثلة، ومثلها المباحث الفدرالية.

وعقب الهجمات الإرهابية التي تعرضت لها الولايات المتحدة الأمريكية في الحادي عشر من سبتمبر ٢٠٠١ م، وفي أجواء ترقب وتحسب دوليين من حدوث هجمات إرهابية متوقعة، الأمر الذي أدى إلى إجتماع ثلاثين دولة وإلى التوقيع على أول اتفاقية دولية لمكافحة الإجرام المعلوماتي في العاصمة المجرية بودابست عام ٢٠٠١م.

وعليه يمكن القول إن الإرهاب الإلكتروني يستخدم الأساليب الحديثة التكنولوجية، والتي تتضمن الإمكانيات التقنية، وتعتمد بالأساس على شبكات المعلوماتية، وذلك بقصد ترويع الأفراد من خلال تهديدهم أو إلحاق الضرر الفعلي بهم.

ويتميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في إستخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.

كما يتميز الإرهاب الإلكتروني عن غيره بسهولة تنفيذه فعلى سبيل المثال إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإجرام والإرهاب وتبادل الآراء والأفكار والمعلومات صعبا في الواقع، فإنه عن طريق الشبكات المعلوماتية تسهل هذه العملية كثيراً، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين، ويتبادلوا الحديث والإستماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا لهم أتباعا وأنصارا عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات

وغرف الحوار الإلكترونية.

وعلى الرغم من أن البريد الإلكتروني(E-mail) أصبح من أكثر الوسائل إستخداماً في مختلف القطاعات, وخاصة قطاع الأعمال؛ لكونه أكثر سهولة وأمنا وسرعةً لإيصال الرسائل، إلا أنه يعدُّ من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال إستخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، بل إن كثيراً من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها، ويقوم الإرهابيون كذلك بإستغلال البريد الإلكتروني والإستفادة منه في نشر أفكارهم والترويج لها، والسعي لتكثير الأتباع والمتعاطفين معهم عبر الرسائل الإلكترونية.

تعريف الإرهاب السيبراني:

بالرغم من عدم وجود تعريف دقيق لمفهوم الإرهاب السيبراني، إلا أن هناك العديد ممن قام بتعريفه، على سبيل المثال: حميس لويس عرف الإرهاب السيبراني بأنه: ”إستخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية، مثل: الطاقة، والنقل، بهدف ترهيب الحكومة والمدنيين“.

كما عرفه البعض بأنه ”إستخدام أنظمة تكنولوجيا المعلومات لمهاجمة البنى التحتية الحيوية أو أنظمة الحكومات والمؤسسات العامة، بهدف

الإكراه والتخويف"، ومكتب التحقيقات الفيدرالي عرف الإرهاب السيبراني بأنه الهجوم المتعمد ذو الدوافع السياسية ضد أنظمة المعلومات، وبرامج الكمبيوتر، والبيانات المخزنة من قبل مختلف الفاعلين.

وسائل الإرهاب السيبراني:

أما عن وسائل الإرهاب السيبراني، فهي البريد الإلكتروني، ويعد من أبرز وسائل الإرهاب السيبراني، حيث يستخدم البريد الإلكتروني في التواصل بين الإرهابيين، وتبادل المعلومات معهم، وإنشاء مواقع إنترنت، ولقد سهلت على المنظمات والجماعات الإرهابية توسيع نشاطهم من خلال تبادل الأفكار والمعلومات، وإختراق وتدمير المواقع، وتتم عملية الإختراق السيبراني عن طريق تسريب البيانات الرئيسية والرموز الخاصة بين برنامج شبكة الإنترنت، وتدمير المواقع، وهو الدخول غير المشروع بهدف التخريب ونشر وسائل تشيد بالإرهاب.

طرق التهديدات السيبرانية:

هناك أربع طرق رئيسة تهدد الأمن السيبراني تتمثل في الآتي:

الطريقة الأولى: هجوم الحرمان من الخدمة، حيث يتم إطلاق خدمة كبيرة من الطلبات على خوادم الضحية بصورة تفوق قدرة الخادم، أو الجهاز على معالجتها والإستجابة لها، مما يؤدي إلى توقيفه بصورة جزئية أو كلية، أو إبطاء عمله، وهذا ما يسبب ضرراً للمستخدم النهائي، وهو

هجوم يهدف إلى تعطيل قدرة الهدف على تقديم الخدمات المعتادة، وذلك عن طريق إعتراف جهاز الحاسب الآلي للخدمة، وهذه الطريقة تستخدم بطبيعة الحال ضد مواقع الإنترنت أو البنوك ، أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.

الطريقة الثانية: فهي إتلاف المعلومات أو تعديلها، ويقصد بهذه الطريقة الوصول إلى معلومات الضحية عبر شبكة الإنترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات المهمة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية، خاصة إذا كانت خططاً عسكرية أو خرائط سرية.

الطريقة الثالثة: هي التجسس على الشبكات، ويقصد بها الوصول غير المصرح، والتجسس على شبكات الضحية دون تدمير أو تغيير في البيانات، والهدف منها الحصول على معلومات قد تتعلق بالأمن القومي للبلاد.

الطريقة الرابعة: هي تدمير المعلومات، في هذه الطريقة يتم مسح وتدمير كامل لأصول المعلومات، والبيانات الموجودة على الشبكات، ويصطلح عليه ''تهديد لسلامة المحتوى ''، ويعني تغيير في البيانات، سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

أسباب الإرهاب السيبراني:

١- إنخفاض تكلفة الآليات الإلكترونية مقارنة بالأدوات التي تستخدم بالإرهاب التقليدي، ففي الإرهاب السيبراني يحتاج الإرهابي جهاز إلكتروني وخط إنترنت، أما الإرهاب التقليدي يحتاج شقة أماكن تدريب وسيارات ..الخ

٢- غياب السيطرة والرقابة على الشبكة المعلوماتية من أهم أسباب إنتشار الإرهاب السيبراني.

٣- ضعف بنية الشبكات المعلوماتية وقابليتها للإختراق، وهذا بطبيعة الحال يوفر للإرهابيين طريقا لتحقيق أهدافهم بسهولة.

٤- غياب الحدود الجغرافية في الفضاء الإلكتروني يعد فرصة مناسبة للإرهابيين.

المطلب الثاني
مفهوم الأمن القومي

على الرغم من أن مصطلح الأمن القومي قد شاع بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، وبخاصة بعد معاهدة وستفاليا عام ١٦٤٨ التي أسست لولادة الدولة القومية أو الدولة – الأمة Nation – State وشكلت حقبة الحرب الباردة الإطار والمناخ اللذين تحركت فيهما محاولات صياغة مقاربات نظرية وأطر مؤسساتية وصولاً إلى إستخدام تعبير ''إستراتيجية الأمن القومي''، وسادت مصطلحات الحرب الباردة مثل الإحتواء والردع والتوازن والتعايش السلمي كعناوين بارزة في هذه المقاربات بهدف تحقيق الأمن والسلم وتجنب الحروب المدمرة التي شهدها النصف الأول من القرن العشرين.

نشأت تبعاً لذلك مؤسسات أكاديمية مهتمة بمسائل الأمن القومي: مصادره، مقوماته، إجراءات ضمان حمايته، من معاهد ومراكز بحث تنتمي إلى جامعات ومؤسسات علمية وإعلامية ومجلات متخصصة وإدارات مؤسسات مرتبطة بالقرار السياسي الرسمي، ويشكل مجلس الأمن القومي في الولايات المتحدة الأمريكية النموذج الأول والأمثل لهذه المؤسسات، حيث جسّد هذا المجلس التعريف الذي طرحه والتر ليبمان عن الأمن القومي بأنه (قدرة الدولة على تحقيق أمنها بحيث لا تضطر إلى التضحية بمصالحها المشروعة لتفادي الحرب، والقدرة على حماية تلك المصالح إذا ما اضطرت عن طريق الحرب).

وقد بدأ التشكيل التنظيمي المؤسسي لمصطلح الأمن القومي بصدور قانون الأمن القومي لعام ١٩٤٧ عن الكونجرس الأمريكي، أما بقية

دول العالم فقد وضعت عنواناً آخر هو ''الدراسات الإستراتيجية'' على الأدبيات التي عالجته بوصفها إجتهادات في التخطيط السياسي النشط حول المستقبل، بدلاً من إجتهادات تعني ضمنياً محاولة لصياغة أجوبة أو ردود فعل بقصد حماية السيادة.

وكأي مصطلح أو مفهوم، فإن مفهوم الأمن القومي لا يمكن التوصل إلى تحديد دقيق له خارج نطاق المكان والزمان الذي يتحرك من خلاله، وهو يخضع دائماً للتعديل والتطوير إنسجاماً مع المتغيرات والعوامل التي تؤثر في بروزه إلى مسرح التداول.

وهكذا أصبح الأمن القومي فرعاً جديداً في العلوم السياسية، حيث إمتلك ثقافة وتوفرت له المادة والهدف العلمي (تحقيق الأمن) وإمكانية الخضوع لمناهج بحث علمية، بالإضافة إلى كونه حلقة وصل بين علوم عديدة، فالأمن القومي ظاهرة مركبة متعددة الأبعاد تربط في دراستها بين علوم الإجتماع والإقتصاد والعلاقات الدولية ونظم الحكم وغيرها، كما تتطلب الإستفادة من المناهج المختلفة وقدراً أكبر من التكامل المنهاجي.

تعريف الأمن القومي:

وللأمن القومي العديد من التعريفات، فقد عرفه "تريجر وكرننبرج" بأنه: ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية.

وعرفه "هنري كيسنجر" بأنه: أية تصرفات يسعى المجتمع – عن طريقها – إلى حفظ حقه في البقاء.

أما "روبرت ماكنمارا فيرى": بأن الأمن القومي هو التنمية، وبدون تنمية لا يمكن أن يوجد أمن، والدول التي لا تنمو في الواقع، لا يمكن

ببساطة أن تظل آمنة.

تعريف الأمن القومي اليمني:

الأمن القومي اليمني: عبارة عن مجموعة الإجراءات والسياسات التي تقوم بها القيادات السياسية الدستورية في الجمهورية اليمنية في حدود طاقتها وإمكانياتها لحماية البلاد وتأمين سلامتها وأمنها وصيانة سيادتها وإستقلالها ووحدتها والحفاظ على قيمها ومنجزاتها الوطنية من أي تهديد داخلي أو عدوان خارجي وذلك من خلال إعداد سياسة تأخذ في الإعتبار المتغيرات الإقليمية والدولية.

وفي الجمهورية اليمنية، أصدر القرار الجمهوري رقم (٢٦٢) لسنة ٢٠٠٢م بإنشاء جهاز للأمن القومي للجمهورية اليمنية، وبحسب ما ورد في قرار الإنشاء فإن المهام التي أنيطت بالجهاز على النحو التالي:-

١- رصد وجمع وتوفير وتحليل المعلومات الإستخباراتية عن كافة المواقف والأنشطة المعادية الموجهة من الخارج التي تشكل تهديداً للأمن القومي للبلاد وسيادتها ونظامها السياسي ومركزها الإقتصادي والعسكري وتقديم الآراء والمقترحات المناسبة لمواجهتها والتعامل معها.

٢- جمع وتوفير المعلومات الإستخباراتية لكل ما يتصل بشؤون وقضايا الأمن القومي للجمهورية اليمنية في مختلف المجالات.

٣- متابعة الأنشطة والمواقف ذات الصلة بسيادة البلاد وأمنها القومي وسياستها الخارجية وتقديم التقارير والتحليلات اللازمة مشفوعة بالمقترحات والملاحظات المناسبة.

٤- تلقي التقارير والتحليلات والمعلومات الإستخباراتية من مختلف المصادر ودراستها ورفعها مشفوعة بالرأي.

٥- دراسة وتحليل البحوث والدراسات السياسية والإقتصادية والإجتماعية والثقافية والأمنية الصادرة عن الهيئات والمؤسسات الأجنبية ومعرفة مدى تأثيرها على الأمن القومي.

٦- كشف ومكافحة الأنشطة التخريبية المعادية للأمن القومي وتأمين حماية حدود البلاد وجزرها من أي إختراق للعناصر المعادية الموجهة من الخارج.

٧- رصد وجمع المعلومات عن كافة الأنشطة التجسسية الموجهة بكافة أشكالها وصورها وأغراضها والعمل على كشفها ومحاربتها.

٨- تأمين حماية القوات المسلحة والأمن وغيرها من مؤسسات ومرافق الدولة والبعثات الدبلوماسية والقنصلية للجمهورية اليمنية في الخارج من أية إختراقات معادية للأمن القومي والمحافظة على أسرار الدولة السياسية والعسكرية والإقتصادية.

٩- إتخاذ التدابير والإجراءات الكفيلة بالحفاظ على أمن وحماية مصالح الجمهورية في الخارج بالتنسيق مع وزارة الخارجية.

١٠- تعزيز وتطوير علاقات التعاون مع الأجهزة والهيئات المماثلة في البلدان الشقيقة والصديقة وتبادل المعلومات والخبرات معها بما يحقق المصالح الوطنية العليا للبلاد.

١١- تأهيل وتدريب العاملين بالجهاز والسعي المستمر لتطوير قدراتهم ومداركهم العلمية والعملية وبما يكفل رفع مستوى أدائهم.

١٢- إعداد التقارير والتحليلات اللازمة تبعاً لمستجدات العمل الإستخباري القومي ومستوى تنفيذ المهام ورفعها أولاً بأول.

المطلب الثالث

تأثير الإرهاب السيبراني على الأمن القومي

للإرهاب الإلكتروني تاثيرات عدة على الأمن القومي للدول وتتمثل في الاتي:

أولًا: سبّب الإرهاب الإلكتروني العديد من المخاطر والتهديدات للأمن القومي للدولة، سواء من خلال أساليب عمله مثل التجسس الإلكتروني والهجوم الإلكتروني أو من خلال النتائج المادية التي يحدثها؛ فعلى المستوى العسكري أدّى الإرهاب الإلكتروني إلى تصاعد المخاطر السيبرانية، خاصة مع قابلية المنشآت الحيوية في الدولة للهجوم، وبالتالي التأثير في وظائف تلك المنشآت والتحكم في تنفيذ هذه الهجمات يُعدان أداة استراتيجية، ولعب الإرهاب الإلكتروني دورًا مهمًّا في عسكرة الفضاء الإلكتروني، وبالتالي تصاعدت القدرات في سباق التسلح السيبراني وتبني سياسات دفاعية سيبرانية في مجال تطوير أدوات الحرب الإلكترونية داخل الجيوش الحديثة، ويذكر أن الإرهاب الإلكتروني عمل على إختراق المخططات العسكرية للدولة، ممّا ساعد على التعرف على طبيعة القوة العسكرية للدولة وتكتيكها العسكري، وبالتالي ذلك يساعد على التحكم في مواجهة الدول المستهدفة، سواء في ميدان الحرب التقليدي أو في الفضاء الإلكتروني.

ثانيًا: على المستوى الإقتصادي، قد تستهدف الهجمات الإلكترونية

توقف الإنترنت كليًّا في الدولة المستهدفة، مما يؤدي إلى توقف المعاملات البنكية ومعاملات الحكومة الإلكترونية وسرقة أرقام وتفاصيل بطاقات الائتمان التي يتم التسوق بها عبر الإنترنت، مما ينتج عن ذلك تعطل تدفق الأموال في الدولة، وبالتالي توقف أهم القطاعات في الدولة مثل الصناعة وغيرها من قطاعات الدولة.

وعلى المستوى النفسي؛ قد تستهدف الهجمات الإلكترونية إحداث حالة من الهلع في الدولة؛ مثل إختراق المواقع الإلكترونية وإعلان حالة الطوارئ، مما يثير القلق لدى المواطنين ويتسبب في إحداث حرب نفسية.

ثالثًا: على المستوى الثقافي، قد يستهدف الإرهاب الإلكتروني مسخ هوية الدولة من خلال الترويج لأفكار الدولة المهاجمة بأساليب تستهدف شباب الدولة وتؤثر على أفكاره ومعتقداته، وهذا ما يُعرف بالغزو الثقافي الذي يستهدف إختراق البنية الفكرية للمجتمعات من خلال إختراق العقول عبر زرع أفكار تُدمّر الإبداع وتُعرقل التنمية الشاملة في الدولة، وهذا ما تستخدمه العديد من الفواعل غير الدولية؛ مثل التنظيمات الإرهابية التي تستهدف الشباب وتجعله يتخذ مسلكًا وطريقًا ضد دولته، وكل هذا يتم عن طريق مواقع التواصل الاجتماعي والقنوات الفضائية.

رابعًا: على المستوى السياسي، قد يستهدف الإرهاب الإلكتروني إثارة الفتن في الدولة وشحن الشعب ضد السلطة الحاكمة وخطابات بث الكراهية من خلال مُخاطبة الشعب بأن هناك العديد من المخاطر التي تُحيط بالدولة، وأن السلطة الحاكمة لا توفر الإحتياجات الأساسية

للشعب، وكذلك مُطالبة شعب الدولة المستهدفة بالحصول على حقوقه المنهوبة، مما يؤدي إلى خروج الشعب إلى مظاهرات وقد تتطور لثورات غير سلمية هدفها التخريب وتدمير الدولة المستهدفة، وكل ذلك يكون بفعل منصات التواصل الإجتماعي، ولعب هذا الهدف دوره في ثورات الربيع العربي عام ٢٠١١ التي تسببت في سقوط أنظمة حُكم العديد من حُكام الدول العربية، بل هناك دول لم تستطِع إسترجاع عافيتها بعد هذه الثورات، مما جعلها مناطق تنافس بين الدول الكُبرى بل وجعلت التنظيمات الإرهابية من هذه الدول مكانًا لها.

وبذلك لم تعد القوة العسكرية وحدها هي المهدد الوحيد للدول، بل أصبح إمتلاك الدول للقوة الإلكترونية يُمثل خطرًا أكبر على الدول المستهدفة، ومن هنا جاء التحول في مفهوم الأمن، بحيث لم يعد أمن الدولة القومي مُقتصرًا على الأمن العسكري، بل أصبح هناك الأمن القومي السياسي، والذي يتلخص في المحتوى الأمني للبيانات الرقمية والمعلومات الإلكترونية التي تخص الأحزاب في الدولة، إضافةً إلى المعلومات التي تتعلق بالبرلمانات وأجهزة الدولة السيادية، هي كلها معلومات حساسة، قد يؤدي العبث بها لحروب أهلية داخل الدولة، وكذلك الأمن القومي الفكري والثقافي والذي يُمثل ذروة الإنتاج الفكري لأي دولة، إذ قد يُسهم في رفع أو خفض مظاهر الأمن القومي للدولة، كالمظهر المادي المتعلق بإستقرار المواطنين أو رفع الهواجس الأمنية في الدولة.

ونظرًا لتعرض المنظومة الإقتصادية والعلمية في الدولة لمثل هذه الحروب كان

لا بد من وجود الأمن القومي الإقتصادي، حيث إنه أكثر القطاعات الأمنية عرضةً للهجمات الإلكترونية؛ نظرًا لتحول الإقتصاد العالمي لإقتصاد رقمي معتمد على تكنولوجيا المعلومات، وبالتالي تعرض تلك المنظومة لمثل هذه الهجمات قد يتسبب في خسائر إقتصادية وقومية هائلة، وأيضًا الأمن القومي العلمي والبحثي الذي يتعلق بالبيانات والمعلومات الخاصة بالمؤسسات البحثية والعلمية والجامعات والتي تُشكل ثروة قومية مستقبلية تحوي العديد من الإكتشافات وبراءة الإختراع المعرضة للسرقة عن طريق القرصنة الإلكترونية.

وهناك العديد من الهجمات الإلكترونية التي كان لها دور فعال في إدارة التفاعلات على الساحة العالمية خلال السنوات الأخيرة ومنها:

– عام ٢٠١٩ تعرضت روسيا لهجوم إلكتروني أصاب شبكتها الكهربائية، وذكرت صحيفة ''نيويورك تايمز'' أن متسللين أمريكيين قاموا بوضع برامج ضارة قادرة على تعطيل الشبكة الكهربائية الروسية، مما أدى لتخصيص مبالغ كبيرة لهذه الأعمال وهي المبالغ التي كانت مُخصصة في الأساس لمكافحة الإرهاب والحروب الأمريكية.

– الهجمات الإلكترونية بين روسيا وأوكرانيا، حيث تعرضت وزارة الطاقة الأوكرانية عام ٢٠١٥ لهجوم إلكتروني مُنسق على شبكة الكهرباء الأوكرانية، وأوضحت التحريات أن متسللين إستخدموا شركة إنترنت مقرها روسيا قاموا بهذا الهجوم، مما تسبب في إنقطاع الكهرباء، وأعتبرت هذه الحادثة أول إنقطاع للكهرباء ناجم عن هجوم إلكتروني.

– سلسلة الهجمات التي وقعت من روسيا ضد أوكرانيا عام ٢٠١٧ حول شبه جزيرة القرم، والتي إستهدفت البنوك والوزارات والصحف وشركات الكهرباء، بل تم فيها إستخدام برمجيات خبيثة من نوع بيتا، مما نتج عنه تعطيل أنظمة المعلومات وتعطيل أعمال الشركات الحكومية والخاصة والمطالبة بدفع فدية بالعملة الإلكترونية البيتكوين التي لا يمكن تعقبها.

قالت شركة مايكروسوفت وفقاً لأحدث تقارير لها، إن أكثر من نصف الهجمات الإلكترونية فى العام الماضي نشأت من روسيا، ووفقًا لتقرير الدفاع الرقمى السنوى للشركة، ٥٢ في المئة من محاولات القرصنة التي ترعاها الدولة من يوليو ٢٠١٩ ويونيو ٢٠٢٠ كانت روسية الأصل، بينما جاء الربع بالضبط خلال هذه الفترة الزمنية من إيران، و١٢ في المئة من الصين و ١١ في المئة المتبقية من كوريا الشمالية ودول أخرى.

وكشفت مايكروسوفت أن الولايات المتحدة تحملت العبء الأكبر من الهجمات الإلكترونية في العام الماضي ، تليها المملكة المتحدة، بينما أكثر من ثلثي – ٦٩ في المئة – من إشعارات NSN المرسلة من قبل Microsoft من يوليو ٢٠١٩ إلى يونيو ٢٠٢٠ كانت إلى عملاء في الولايات المتحدة.

تم إرسال ١٩ في المئة إلى عملاء في المملكة المتحدة، تليها ٥ في المئة فى كندا، و ٤ في المئة فى كوريا الجنوبية و ٣ في المئة في المملكة العربية السعودية.

كانت إيران، التي تمثل ثاني أكبر عدد من محاولات الإختراق بعد روسيا، مصدراً لزيادة النشاط السيبراني المدعوم من الدولة، ففي فترة ٣٠ يوما بين أغسطس وسبتمبر ٢٠١٩، لاحظت Microsoft أن متسللين مقرهم إيران يهاجمون ٢٤١ حسابا لعملاء Microsoft.

وتملك روسيا، مجموعة من الأدوات الإلكترونية الهجومية التي يمكن أن تستخدمها ضد الشبكات الأمريكية، ويمكن أن تتراوح الهجمات من مستوى منخفض لرفض الخدمة إلى الهجمات "المدمرة" التي تستهدف البنية التحتية الحيوية.

ولطالما إتهمت الولايات المتحدة نظيرتها روسيا، بتنفيذ الأخيرة هجمات على مرافق أمريكية حيوية، فيما تعي واشنطن أن قدرة روسيا على إجراء هجمات إلكترونية مدمرة في الوطن ربما تظل مرتفعة للغاية.

وفي عام ٢٠٢١، قالت الولايات المتحدة إن مجرمي الإنترنت المتمركزين في روسيا تسببوا في هجومين إلكترونيين من أكثر الهجمات الإلكترونية تدميراً في الذاكرة الحديثة.

حيث كانت شركة كولونيال بايبلاين ضحية لهجوم برمجيات الفدية في مايو ٢٠٢١، مما أدى إلى إغلاق العمليات وتسبب في إنقطاعات واسعة النطاق في جميع أنحاء البلاد.

كما تتهم واشنطن موسكو، بإختراق شركة "SolarWinds" في أواخر

عام ٢٠٢٠، حيث تقول الولايات المتحدة إن مجرمي الإنترنت المدعومين من روسيا تمكنوا من الوصول إلى ١٠ وكالات حكومية أمريكية، بما في ذلك وزارة الأمن الداخلي ووزارة التجارة.

ووفق مجلة فوربس، تتجاوز الهجمات الإلكترونية الأخيرة خلال العشرين عاما الماضية، ضد ١٨٠٠٠ مستخدم من القطاعين العام والخاص الأمريكي، حدود التجسس التقليدي؛ "بل إنها أعمال عدوان إلكتروني من قبل روسيا ضد الأنظمة الأمريكية إستمرت لمدة عشرين عامًا".

وبدأت الهجمات الروسية على أمريكا في عام ١٩٩٦ بهجوم Moonlight Maze، وهي واحدة من أولى حملات التجسس السيبراني التي ترعاها موسكو، بحسب فوربس.

حينها تم إلقاء اللوم على روسيا في هجمات Moonlight Maze، والتي تضمنت سرقة كمية هائلة من المعلومات السرية من العديد من الوكالات الحكومية بما في ذلك وزارة الطاقة ووكالة ناسا ووزارة الدفاع الأمريكية.

وفي عام ٢٠٠٨، بدأت مجموعة قرصنة روسية تُدعى تورلا، بمهاجمة الأنظمة العسكرية الأمريكية بإستخدام الخداع والأبواب الخلفية والجذور الخفية وإصابة المواقع الحكومية.

في حينها أيضا، تم إلقاء اللوم على المخابرات الروسية في الهجوم؛ بينما

في عام ٢٠١٧، تمكن أربعة باحثين كمبيوتر من Kaspersky Labs و Kings College في لندن من الحصول على خادم الطرف الثالث المستخدم لتوجيه هجمات Moonlight Maze؛ وأظهرت النتائج أن روسيا هي وراء ذلك.

وقبل عدة سنوات، قامت مجموعة قرصنة روسية أخرى تعرف بإسم APT-٢٨، بإختراق اللجنة الوطنية الديمقراطية، وكذلك البيت الأبيض والبرلمانين الألماني والنرويجي، ومنظمة الأمن والتعاون في أوروبا، والصحفيين.

The impact of cyber terrorism on national security

Preparation
Brigadier General. Dr. Jalal Fadl Muhammad Al-Awdi

The impact of cyber terrorism on national security

Preparation
Brigadier General. Dr. Jalal Fadl Muhammad Al-Awdi

introduction

In light of the information technology revolution, various terrorist and extremist groups rushed to own sites on the Internet, especially social networks, some of which have more than one site and in more than one language, in order to introduce the organization, its history, founders and activities, its political and social backgrounds, its intellectual and political goals, and the latest news. and attacking his opponents from the intellectuals and scholars, and from the governments and the security services.

In 1998, the number of terrorist websites on the World Wide Web was less than 20, while today it is in the thousands, apart from tens of thousands of pages on social networks. Safe, easy and inexpensive means of communication around the world have made it difficult to monitor and limit their activity.

For example, in recent years, ISIS has been able to support its electronic capabilities by integrating its (cyber) arms such as: the "Ghost Caliphate", the "Sons Caliphate Army", the "Caliphate Cyber Army", and Kalashnikov E-Security in The United Cyber Caliphate Hacker Group.

A group of ISIS-affiliated hackers managed to penetrate some of the network's websites to defame them and spread extremist propaganda, such as the sites of the British Ministry of Health, the Royal Malaysian Police, Malaysia Airlines, the French TV5 network and its affiliated stations, and the US Central Command.

Accordingly, we will divide this research into the following demands:

The first requirement: the concept of cyber terrorism.

The second requirement: the concept of national security.

The third requirement: the impact of cyber terrorism on national security.

The first requirement

cyber security concept

The first appearance of the concept of cyber terrorism was in the eighties of the twentieth century, when Barry Collin defined it as “an electronic attack whose purpose is to threaten or attack governments, in pursuit of political, religious or ideological goals, and that the attack must have a devastating and disruptive effect.” equivalent to physical acts of terrorism."

But electronic terrorism did not appear officially, except when US President Bill Clinton formed the Sensitive Infrastructure Protection Authority in 1996 , and the first conclusion of this body was that the sources of electric power and communications in addition to computer networks are absolutely necessary for the survival of the United States, and since That these facilities rely heavily on digital information, they will be the first target for any terrorist attacks targeting the security of the United States, and in the wake of that, all government agencies in the United States, have established their own bodies and centers, to deal with the possibilities of electronic terrorism, so the Central Intelligence Agency established The Center for Information Wars, and hired a thousand information security experts, and a -24hour strike force to confront electronic terrorism. The US Air Force took similar steps, as did the FBI.

Following the terrorist attacks on the United States of America on 11 September 2001, and in an atmosphere

of international anticipation and anticipation of expected terrorist attacks, which led to the meeting of thirty countries and the signing of the first international agreement to combat cybercrime in the Hungarian capital Budapest in 2001. .

Accordingly, it can be said that electronic terrorism uses modern technological methods, which include technical capabilities, and mainly rely on information networks, with the aim of intimidating individuals by threatening them or causing actual harm to them.

Electronic terrorism is distinguished from other types of terrorism by the modern way of using information resources and electronic means brought by the technology civilization in the information age, so electronic systems and information infrastructure are the target of terrorists.

What distinguishes electronic terrorism from others is its ease of implementation. For example, if terrorists and criminals meet in a particular place to learn the methods of crime and terrorism and exchange opinions, ideas and information is actually difficult, then through information networks this process is greatly facilitated, as several people can meet in multiple places. At a certain time, they exchange talk and listen to each other over the information network, but they can gather followers and supporters by spreading their ideas and principles through websites, forums and electronic dialogue rooms.

Although e-mail has become one of the most widely used means in various sectors, especially the business sector; Because it is easier, safer and faster to deliver messages, it is considered one of the greatest means used in electronic terrorism, through the use of e-mail to communicate between terrorists and exchange information among them. Indeed, many of the terrorist operations that have occurred recently were e-mail as a means One of the means of exchanging information and transferring it between those who carry out terrorist operations and those who plan them. Terrorists also exploit e-mail and take advantage of it to spread and promote their ideas, and seek to increase followers and sympathizers through e-mails.

Definition of cyber terrorism:

Although there is no precise definition of the concept of cyber terrorism, there are many who defined it, for example: Hamas Lewis defined cyber terrorism as: "The use of computer network tools to destroy or disrupt national infrastructure, such as: energy and transportation, with the aim of intimidating government and civilians.

Some also defined it as "the use of information technology systems to attack critical infrastructure or systems of governments and public institutions, with the aim of coercion and intimidation." The Federal Bureau of Investigation defined cyber terrorism as the deliberate, politically motivated attack against information systems, computer programs, and data stored by various actors.

Cyber terrorism means:

As for the means of cyber terrorism, it is e-mail, and it is one of the most prominent means of cyber terrorism, where e-mail is used to communicate between terrorists, exchange information with them, and create Internet sites, and it has made it easier for terrorist organizations and groups to expand their activity through the exchange of ideas and information, penetration and destruction Sites, and the process of cyber penetration by leaking key data and private codes between the Internet program, and destroying sites, which is the illegal entry with the aim of sabotage and the dissemination of means that praise terrorism.

Methods of cyber threats:

There are four main ways that threaten cyber security, as follows:

The first method: a denial of service attack, in which a large service of requests is launched on the victim's servers in a way that exceeds the ability of the server or the device to process and respond to it, which leads to stopping it partially or completely, or slowing down its work, and this causes harm to the end user, It is an attack aimed at disrupting the target's ability to provide the usual services, by recognizing the service's computer, and this method is used, of course, against websites, banks, or institutions in order to influence them or to pay a ransom.

The second method: it is to destroy or modify the information, and this method is intended to access the victim's information via the Internet or private networks, and to carry out the process of modifying the important data without the victim discovering it. or secret maps.

The third method: is network espionage, which means unauthorized access, and spying on the victim's networks without destroying or changing the data, and the aim is to obtain information that may relate to the country's national security.

The fourth method: is the destruction of information. In this method, information assets and data on networks are completely erased and destroyed, and it is termed as a "threat to the integrity of the content", and it means a change in the data, whether by deletion or destruction by unauthorized persons.

Causes of cyber terrorism:

1. The low cost of electronic mechanisms compared to the tools that are used in traditional terrorism. In cyber terrorism, the terrorist needs an electronic device and an internet line, while traditional terrorism needs apartments, training places, cars....etc.

2. The absence of control and oversight over the information network is one of the most important reasons for the spread of cyber terrorism.

3. The weak structure of information networks and

their vulnerability to penetration, and this of course provides terrorists with a way to achieve their goals easily.

4. The absence of geographical borders in cyberspace is a suitable opportunity for terrorists.

The second requirement

The concept of national security

Although the term national security was popularized after World War II, its roots go back to the seventeenth century, especially after the Treaty of Westphalia in 1648, which established the birth of the nation-state or the nation-state and the Cold War era formed the framework and climate in which it moved Attempts to formulate theoretical approaches and institutional frameworks, leading to the use of the term "national security strategy." Cold War terms such as containment, deterrence, balance and peaceful coexistence prevailed as prominent titles in these approaches with the aim of achieving security and peace and avoiding the devastating wars witnessed in the first half of the twentieth century.

Accordingly, academic institutions concerned with national security issues arose: its sources, its components, and procedures to ensure its protection, from institutes and research centers belonging to universities, scientific and media institutions, specialized magazines, and administrations of institutions linked to the official political decision. The National Security Council in the United States of America is the first and ideal model for these institutions. , where this council embodied the definition put forward by Walter Lippmann about national security as (the ability of the state to achieve its security so that it does not have to sacrifice its legitimate interests to avoid war, and the ability to protect those

interests if forced by war).

The institutional organizational formation of the term national security began with the issuance of the National Security Act of 1947 by the US Congress, while the rest of the world has put another title, “Strategic Studies” on the literature that treated it as jurisprudence in active political planning about the future, rather than jurisprudence that implied an attempt To formulate answers or reactions with the intent of protecting sovereignty.

Like any term or concept, the concept of national security cannot be accurately defined outside the scope of the place and time through which it moves, and it is always subject to modification and development in line with the variables and factors that affect its emergence to the deliberative stage.

Thus, national security became a new branch in political science, as it possessed a culture, provided it with a material and a scientific objective (achieving security) and the possibility of submitting to scientific research methods, in addition to being a link between many sciences. International relations, governance systems, and others, as well as taking advantage of different curricula and a greater degree of methodological integration.

Defining National Security:

National security has many definitions, as "Treasure

and Krnenberg" defined it as: that part of government policy that aims to create conditions conducive to the protection of vital values.

And "Henry Kissinger" defined it as: any behavior by which society seeks - through which - to preserve its right to survival.

As for "Robert McNamara", he believes that national security is development, and without development there can be no security, and countries that do not actually develop, cannot simply remain secure.

Yemen National Security Definition:

Yemeni National Security: It is a set of procedures and policies undertaken by the constitutional political leaders in the Republic of Yemen within the limits of their capabilities and capabilities to protect the country, secure its safety and security, maintain its sovereignty, independence and unity, and preserve its national values and achievements from any internal threat or external aggression, through the preparation of a policy that takes into account the Taking into account regional and international variables.

In the Republic of Yemen, Presidential Decree No. (262) of 2002 was issued to establish a National Security Agency for the Republic of Yemen. According to the establishment decision, the tasks assigned to the agency are as follows:-

1. Monitoring, collecting, providing and analyzing intelligence information on all hostile attitudes and activities directed from abroad that pose a threat to the country’s national security, sovereignty, political system, economic and military status, and providing appropriate opinions and proposals to confront and deal with them.

2. Collecting and providing intelligence information for everything related to the national security affairs and issues of the Republic of Yemen in various fields.

3. Follow-up activities and positions related to the country's sovereignty, national security and foreign policy, and submit the necessary reports and analyzes accompanied by appropriate suggestions and observations.

4. Receiving reports, analyzes and intelligence information from various sources, studying them and submitting them together with an opinion.

5. Studying and analyzing political, economic, social, cultural and security research and studies issued by foreign bodies and institutions and knowing the extent of their impact on national security.

6. Detecting and combating subversive activities hostile to national security and ensuring the protection of the country's borders and islands from any penetration of hostile elements directed from abroad.

7. Monitoring and collecting information on all espionage activities directed in all their forms, forms and purposes, and working to detect and combat them.

8. Securing the protection of the armed and security forces and other institutions and facilities of the state and the diplomatic and consular missions of the Republic of Yemen abroad from any intrusions hostile to national security and the preservation of the state's political, military and economic secrets.

9. Take measures and measures to maintain the security and protection of the Republic's interests abroad, in coordination with the Ministry of Foreign Affairs.

10. Strengthening and developing cooperation relations with similar agencies and bodies in brotherly and friendly countries and exchanging information and experiences with them in a way that achieves the country's supreme national interests.

11. Qualifying and training the employees of the Agency and constantly striving to develop their capabilities and scientific and practical awareness in a manner that ensures raising the level of their performance.

12. Preparing the necessary reports and analyzes according to the latest developments in the national intelligence work and the level of implementation of tasks, and submitting them up-to-date.

The third requirement

The impact of cyber terrorism on national security

Cyber terrorism has several effects on the national security of countries, which are as follows:

First : Cyber terrorism has caused many risks and threats to the national security of the state, whether through its methods of operation such as electronic espionage and cyber attack, or through the material consequences it causes; At the military level, cyber terrorism has led to an escalation of cyber risks, especially with the vulnerability of vital facilities in the country to attack, and thus affecting the functions of these facilities and controlling the implementation of these attacks is a strategic tool. Cyber armament and the adoption of cyber defense policies in the field of developing electronic warfare tools within modern armies, and it is mentioned that electronic terrorism worked to penetrate the military plans of the state, which helped to identify the nature of the state's military power and its military tactics, and thus this helps to control the confrontation of the targeted countries, whether In the field of conventional warfare or in cyberspace.

Second : On the economic level, cyber attacks may target the complete shutdown of the Internet in the target country, which leads to the cessation of banking and e-government transactions and the theft of credit card numbers and details that are shopped online,

which results in the disruption of the flow of funds in the country, and thus stops The most important sectors in the country such as industry and other sectors of the state.

on a psychological level; Cyber attacks may aim to cause panic in the country; Such as hacking websites and declaring a state of emergency, which raises concern among citizens and causes psychological warfare.

Third : On the cultural level, electronic terrorism may target distorting the identity of the state by promoting the ideas of the attacking state in ways that target the youth of the state and affect their ideas and beliefs. comprehensive in the state, and this is what many non-international actors use; Such as terrorist organizations that target young people and make them take a course against their state, and all this is done through social media and satellite channels.

Fourth : On the political level, electronic terrorism may aim to stir up sedition in the state and mobilize the people against the ruling authority and hate speeches by addressing the people that there are many dangers surrounding the state, and that the ruling authority does not provide the basic needs of the people, as well as asking the people of the targeted state to obtain On their looted rights, which leads to people going out to demonstrations and may develop into non-peaceful revolutions aimed at sabotaging and destroying the targeted country, and all this is due to social media platforms, and this goal played its role in the Arab Spring

revolutions in 2011 that caused the fall of the regimes of many rulers of countries In fact, there are countries that were unable to recover after these revolutions, which made them areas of competition between the major countries and even made terrorist organizations of these countries a place for them.

Thus, military force alone is no longer the only threat to states. Rather, states' possession of electronic force has become a greater danger to the targeted states, hence the shift in the concept of security, so that the state's national security is no longer limited to military security, but rather there has become a political national security, Which is summarized in the security content of digital data and electronic information related to the parties in the state, in addition to information related to parliaments and sovereign state agencies, all of which are sensitive information, tampering with may lead to civil wars within the state, as well as national intellectual and cultural security, which represents the peak of intellectual production for any A state, as it may contribute to raising or lowering the national security aspects of the state, such as the physical aspect related to the stability of citizens or raising security concerns in the state.

Since the economic and scientific system in the country has been exposed to such wars, it was necessary to have national economic security, as it is the security sector most vulnerable to electronic attacks; Due to the transformation of the global economy into a digital

economy dependent on information technology, and thus the exposure of that system to such attacks may cause huge economic and national losses, as well as national scientific and research security that relates to data and information of research and scientific institutions and universities, which constitute a future national wealth containing many discoveries and innocence Invention vulnerable to theft by electronic hacking.

There are many cyber attacks that have had an effective role in managing interactions on the global scene in recent years, including:

– In 2019, Russia was subjected to a cyber attack that hit its electrical network, and the New York Times reported that American hackers had developed malicious programs capable of disrupting the Russian electrical network, which led to the allocation of large sums of money to these works, amounts that were originally intended to combat terrorism and American wars.

- Cyber-attacks between Russia and Ukraine, where the Ukrainian Ministry of Energy was subjected to a coordinated cyber-attack in 2015 on the Ukrainian electricity network. electronic.

– The series of attacks that took place from Russia against Ukraine in 2017, around the Crimea, which targeted banks, ministries, newspapers and electricity companies, and even used beta malware, which resulted in the disruption of information systems, the disruption of the work of government and private companies

and the demand for payment of ransom in electronic currency Bitcoin untraceable.

- According to Microsoft, according to its latest reports, more than half of cyber attacks last year originated from Russia, and according to the company's annual digital defense report, 52 percent of state-sponsored hacking attempts from July 2019 and June 2020 were Russian in origin, while exactly a quarter came from Russia. During this time period from Iran, 12 percent from China and the remaining 11 percent from North Korea and other countries.

- Microsoft revealed that the US bore the brunt of cyberattacks last year, followed by the UK, while more than two-thirds - 69 percent - of NSN notifications sent by Microsoft from July 2019 to June 2020 were to US customers.

19 percent were sent to customers in the United Kingdom, followed by 5 percent in Canada, 4 percent in South Korea and 3 percent in Saudi Arabia.

- Iran, which accounts for the second largest number of hack attempts after Russia, has been a source of increased state-backed cyber activity. In a -30day period between August and September 2019, Microsoft observed that Iran-based hackers were attacking 241 Microsoft customer accounts.

- Russia has an array of offensive cyber tools that it can use against US networks, and attacks can range from

low-level denial of service to "disruptive" attacks that target critical infrastructure.

The United States has long accused its counterpart Russia of carrying out attacks on vital American facilities, while Washington is aware that Russia's ability to conduct devastating cyber attacks at home may remain very high.

In 2021, the United States said Russian-based cybercriminals caused two of the most destructive cyber attacks in recent memory.

Colonial Pipeline was the victim of a ransomware attack in May 2021, which shut down operations and caused widespread outages across the country.

Washington also accuses Moscow of hacking SolarWinds in late 2020, as the US says Russian-backed cybercriminals gained access to 10 US government agencies, including the Department of Homeland Security and the Department of Commerce.

According to Forbes magazine, recent cyber attacks over the past 20 years against 18,000 US public and private users exceed the limits of traditional espionage; Rather, they are acts of cyber aggression by Russia against American regimes that have continued for twenty years.

Russian attacks on America began in 1996 with the Moonlight Maze attack, one of the first cyberespionage campaigns sponsored by Moscow, according to Forbes.

Russia was blamed for the Moonlight Maze attacks, which involved the theft of a massive amount of classified information from several government agencies including the Department of Energy, NASA and the US Department of Defense.

In 2008, a Russian hacking group called Turla began attacking US military systems using deception, backdoors, rootkits and infecting government websites.

At the same time, Russian intelligence was blamed for the attack; While in 2017, four computer researchers from Kaspersky Labs and Kings College in London managed to acquire the third-party server used to direct Moonlight Maze attacks; The results showed that Russia is behind this.

Several years ago, another Russian hacking group known as APT28- hacked the Democratic National Committee, as well as the White House, the German and Norwegian parliaments, the Organization for Security and Cooperation in Europe, and journalists.

L'impact du cyberterrorisme sur la sécurité nationale

Préparation
Général de brigade. Dr / Jalal Fadl Mohammed Al-Oudi

L'impact du cyberterrorisme sur la sécurité nationale

Préparation
Général de brigade. Dr / Jalal Fadl Mohammed Al-Oudi

Introduction

Dans l'ère de la révolution technologique et informatique, les groupes terroristes et extrémistes se sont rués sur leurs propres sites sur Internet, notamment les réseaux sociaux, dont certains ont plusieurs médias et en plusieurs langue, afin de promouvoir leur idéologie, ses histoire, , les activités, les convections politiques et sociaux, et pour cibler leurs (adversaires) comme les intellectuelles , les gouvernements et des services de sécurité.

En 1998, le nombre de ce genre de sites Web terroristes sur le réseau internet était inférieur à 20 sites , alors qu'il se compte aujourd'hui par des milliers. Cela mis à part de dizaines de milliers de pages sur les réseaux sociaux. Un rapport sur les cyberterrorisme a révélé des faits troublants - les terroristes ont bénéficié de systèmes d'information et de communication de haute technologie, qui leur ont fourni des moyens de communication sûrs, faciles et peu coûteux dans le monde entier, ce qui a rendu difficile la surveillance et la limitation de leur activité.

Par exemple, ces dernières années, l'Etat islamique a pu soutenir ses capacités électroniques en intégrant ses (cyber-armés) telles que : le "Ghost Califate", la "Caliphate Cyber Army", " Kalachnikov E-Security" et le " United Cyber Caliphate Hacker Group".

Un groupe de pirates informatiques de l'Etat islamique a réussi à pénétrer dans certains des sites d'Internet pour

les diffamer et diffuser leurs propagande extrémiste, tels que les sites du ministère britannique de la Santé, de la police royale malaisienne, de Malaysia Airlines, du réseau français TV5 et le Commandement central militaire américain.

nous allons traiter ce sujet selon le chèma suivant :

Le Première section : la notion de cyberterrorisme.

Le deuxième section : la notion de sécurité nationale.

le troisième section : l'impact du cyberterrorisme sur la sécurité nationale.

Le Première section

la notion de cyberterrorisme

La première apparition du concept de cyberterrorisme remonte aux années 80 du XXe siècle, lorsque Barry Collin le définit comme « une attaque électronique dont le but est de menacer ou d'attaquer des gouvernements, pour des objectifs politiques, religieux ou idéologiques, et que le cet attaque doit avoir des effets dévastateur et perturbateur, équivants aux actes physiques de terrorisme."

le président américain Bill Clinton a créé autorité de la protection de Infrastructure sensibles, en 1996, et la première conclusion a été que les sources d'énergie électrique et les communications, en plus des réseaux informatiques, sont absolument nécessaires la vie des américaines, pour Étant donné que ces installations dépendent fortement des informations numériques, elles seront la cible principale de toute attaque terroriste visant la sécurité des États-Unis. Par la suite, toutes les agences gouvernementales aux États-Unis ont créé leurs propres agences et centres pour faire face aux possibilités du cyberterrorisme. La Central Intelligence Agency CIA a créé un centre de guerre informatique et a embauché un millier d'experts en sécurité de informatique et une

force de frappe 24h/24h pour lutter contre le terrorisme électronique. L'US Air Force a pris des mesures similaires, tout comme le FBI.

Suite aux attentats terroristes du 11 septembre 2001 aux États-Unis d'Amérique, et dans une atmosphère d'anticipation des attentats, une trentaine de pays ont réuni pour la signature du premier accord international de lutte contre la cybercriminalité au Budapest/Hongrie en 2001.

Le terrorisme électronique se distingue des autres types de terrorisme par la manière moderne d'utiliser les ressources d'information et les moyens électroniques apportée par la civilisation technologique à l'ère de l'information. Par conséquent, les systèmes électroniques et les infrastructures d'information sont la cible des terroristes.

Le terrorisme électronique se distingue aussi par sa facilité de mise en œuvre. Par exemple, si des terroristes et des criminels se rencontrent dans un lieu particulier pour apprendre les méthodes du crime et du terrorisme et échanger des opinions, des idées et des informations est en fait difficile, alors, à travers les réseaux d'information, ce processus grandement facilite, car plusieurs personnes peuvent se rencontrer à plusieurs endroits. À un certain

moment, ils échangent des conversations et s'écoutent sur le réseau d'information, mais ils peuvent rassembler des adeptes et des partisans en diffusant leurs idées et leurs principes à travers des sites Web, des forums et des salles de dialogue électroniques.

Bien que le courrier électronique soit devenu l'un des moyens les plus utilisés dans divers secteurs, en particulier le secteur des affaires, Parce qu'il est plus facile, plus sûr et plus rapide de transmettre des messages, il est considéré comme l'un des plus grands moyens utilisés dans le terrorisme électronique, à travers l'utilisation du courrier électronique pour communiquer entre terroristes et échanger des informations entre eux. Récemment, le courrier électronique est un moyen d'échange et de transfert d'informations entre ceux qui mènent des opérations terroristes et ceux qui les planifient. Les terroristes exploitent et profitent également du courrier électronique pour diffuser et promouvoir leurs idées, et chercher à augmenter les sympathisants par le biais des réseaux sociaux.

La définition du cyberterrorisme :

Jamas Lewis a défini le cyberterrorisme comme : « L'utilisation des outils de réseau informatique pour détruire ou perturber les infrastructures nationales,

telles que : l'énergie et transport, dans le but d'intimider le gouvernement et les civils.

Certains l'ont également défini comme "l'utilisation de systèmes de technologie de l'information pour attaquer des infrastructures ou des systèmes critiques de gouvernements et d'institutions publiques, dans le but de coercition et d'intimidation."

Le FBI, de son côté, a défini le cyberterrorisme comme une attaque délibérée et politiquement motivée contre les systèmes d'information, les programmes informatiques et les données stockées par divers acteurs.

Les Méthodes de cybermenaces :

Il existe quatre types de menacer la cybersécurité : **La première méthode :** une attaque pour priver de service, dans laquelle un grand service de requêtes est lancé sur les serveurs ciblés, d'une manière qui dépasse la capacité du serveur de traiter et à y répondre, ce qui entraîne la suspension partielle ou totale d'un appareil ou ralentir son travail, et cela cause un préjudice à l'utilisateur final, Il s'agit d'une attaque visant à perturber la capacité de la cible à fournir les services habituels et cette méthode est utilisée, bien sûr , contre des sites Internet, des banques ou des institutions dans le but de les influencer ou de leur verser une rançon.

La deuxième méthode : détruire ou à modifier les informations, et cette méthode est destinée à accéder aux informations de la victime/cible à travers Internet ou des réseaux privés, et à effectuer le processus par de modifications des données importantes.

La troisième méthode : est l'espionnage de réseaux, c'est-à-dire l'accès non autorisé et l'espionnage des réseaux de la victime sans détruire ni modifier les données, et le but est d'obtenir des informations pouvant concerner la sécurité nationale du pays.

La quatrième méthode : est la destruction de l'information. Dans cette méthode, l'objectif est de détruire les données sur les réseaux, cela est qualifié de "menace pour l'intégrité du contenu", et cela signifie un changement dans les données , que ce soit par suppression ou destruction par des personnes non autorisées.

Les causes du cyberterrorisme :

1. Le faible coût des mécanismes électroniques par rapport aux outils utilisés dans le terrorisme traditionnel. Dans le cyberterrorisme, le terroriste a besoin d'un appareil électronique et d'une ligne internet, alors que le terrorisme traditionnel a besoin beaucoup de matériels, des moyens, de lieux d'entraînement, de

voitures...etc.

2. Le manque de contrôle sur le réseau d'information .

3. La faible structure des réseaux d'information et leur capacité de pénétration, et cela fournit aux terroristes un moyen d'atteindre facilement leurs objectifs.

4. L'absence de frontières géographiques dans le cyberespace est une bonne opportunité pour les terroristes.

Le deuxième section

la notion de sécurité nationale

le terme sécurité nationale ait été popularisé après la Seconde Guerre mondiale, mais ses racines remontent au XVIIe siècle, en particulier après le traité de Westphalie en 1648, qui a établi la naissance de l'État-nation. l'ère de la guerre froide a formé le cadre et le climat dans lesquels elle évolue Les tentatives de formulation d'une approches théoriques et de cadres institutionnels ont conduit à l'utilisation du terme « stratégie de sécurité nationale ».

En conséquence, des institutions académiques concernées par la question de sécurité nationale ont émergé : ses sources, ses composantes et les procédures pour assurer sa protection, des instituts et des centres de recherche appartenant aux universités, des institutions scientifiques et médiatiques, des revues spécialisées et des administrations des institutions liées à la politique officielle.

Le National Security Council aux États-Unis d'Amérique est le modèle idéal de ces institutions, car ce conseil incarnait la définition avancée par Walter Lippmann de la sécurité nationale comme (la capacité de l'État à assurer sa sécurité afin qu'il ne doit sacrifier ses intérêts légitimes pour éviter la guerre, et sa capacité à protéger ces intérêts si la guerre l'y oblige).

La formation organisationnelle institutionnelle du

concept de la sécurité nationale a commencé avec la publication de la loi sur la sécurité nationale de 1947 par le Congrès américain, tandis que le reste du monde a donné un autre titre, "études stratégiques" pour mentionner la planification politique sur l'avenir, plutôt que la jurisprudence qui impliquait une tentative de formuler des réponses ou des réactions dans le but de protéger la souveraineté.

Comme tout terme ou concept, le concept de sécurité nationale ne peut être défini avec précision en dehors du son contexte géographique et temporelle , il est toujours un sujet à développement en fonction des variables et des facteurs qui affectent son émergence dans le stade de la délibération.

C'est ainsi que la sécurité nationale est devenue une nouvelle branche de la science politique, car elle possédait une culture et avait un objectif matériel et scientifique (atteindre la sécurité) et la possibilité de se soumettre à des méthodes de recherche scientifique, en plus d'avoir un lien entre de nombreuses sciences. systèmes de gouvernance, et autres, ainsi que de tirer parti de différents programmes et d'un plus grand degré d'intégration méthodologique.

Définir la sécurité nationale :

Treasure et Krnenberg" l'a défini comme : cette partie de la politique gouvernementale qui vise à créer des conditions propices à la protection des valeurs vitales. Henry Kissinger l'a défini comme : tout comportement

par lequel la société cherche - à travers lequel - à préserver son droit à la survie.

Quant à Robert McNamara, il estime que la sécurité nationale est le développement. sans développement, il ne peut y avoir de sécurité, et les pays qui ne se développent pas réellement ne peuvent pas simplement rester en sécurité.

Définir la sécurité nationale yéménite :

La Sécurité nationale yéménite , il s'agit d'un ensemble de procédures et de politiques mises en œuvre par les dirigeants politiques constitutionnels de la République du Yémen dans la limite de leurs capacités de protéger le pays, assurer sa sûreté et sa sécurité, maintenir sa souveraineté, son indépendance et son unité, préserver ses valeurs et et ses intérêts nationales de toute menace intérieure ou agression extérieure, à travers l'élaboration d'une politique qui tient compte des situations régionales et internationales.

En République du Yémen, le décret présidentiel n° (262) de 2002 AD a été publié pour établir un appareil de sécurité nationale pour la République du Yémen. Selon la décision d'établissement, les tâches assignées au dispositif sont les suivantes :

1. Surveiller, collecter, fournir et analyser des informations de renseignement sur toutes les attitudes et activités hostiles dirigées de l'étranger qui constituent une menace pour la sécurité nationale, la souveraineté, le

système politique, le statut économique et militaire du pays, et présenter des opinions et des propositions appropriées pour affronter et traiter avec eux.

2. Collecter et fournir des informations de renseignement sur toutes les questions liées aux problèmes de sécurité nationale de la République du Yémen dans divers domaines.

3. Assurer le suivi des activités et des positions liées à la souveraineté, à la sécurité nationale et à la politique étrangère du pays, et soumettre les rapports et analyses nécessaires accompagnés des suggestions et observations appropriées.

4. Recevoir des rapports, des analyses et des informations de renseignement provenant de diverses sources, les étudier et les soumettre avec un avis.

5. Étudier et analyser les recherches et études politiques, économiques, sociales, culturelles et de sécurité émises par des organismes et institutions étrangers et connaître l'étendue de leur impact sur la sécurité nationale.

6. Détecter et combattre les activités subversives hostiles à la sécurité nationale et assurer la protection des frontières et des îles du pays contre toute pénétration d'éléments hostiles dirigés de l'étranger.

7. Surveiller et collecter des informations sur toutes les activités d'espionnage dirigées sous toutes leurs

formes, formes et finalités, et travailler à les détecter et à les combattre.

8. Assurer la protection des forces armées et de sécurité et des autres institutions et installations de l'État et des missions diplomatiques et consulaires de la République du Yémen à l'étranger contre toute intrusion hostile à la sécurité nationale et la préservation des secrets politiques, militaires et économiques de l'État .

9. Prendre des mesures pour préserver la sécurité et la protection des intérêts de la République à l'étranger, en coordination avec le ministère des Affaires étrangères.

10. Renforcer et développer les relations de coopération avec les organes similaires des pays et échanger avec eux des informations et des expériences de manière à atteindre les intérêts nationaux suprêmes du pays.

11. former les employés de l'appareil, développer leurs capacités, leurs connaissances scientifiques et pratiques de manière à assurer l'élévation de leur niveau de performance.

12. Préparer les rapports et les analyses nécessaires en fonction des derniers développements des efforts nationaux, de renseignement, du niveau d'exécution des tâches, et les soumettre à jour.

le troisième section

L'impact du cyberterrorisme sur la sécurité nationale

Le cyberterrorisme a plusieurs effets sur la sécurité nationale des pays, qui sont les suivants :

Premièrement : Le cyberterrorisme a engendré de nombreux risques et menaces pour la sécurité nationale de l'État, que ce soit par ses modes opératoires tels que l'espionnage électronique et la cyberattaque, ou par les conséquences matérielles qu'il engendre.

Au niveau militaire, le cyber-terrorisme a conduit à une escalade des cyber-risques, notamment avec la vulnérabilité des installations vitales du pays aux attaques, affectant ainsi les fonctions de ces installations et le contrôle de la mise en œuvre de ces attaques est un outil stratégique. l'armement et l'adoption de politiques de cyberdéfense dans le domaine du développement d'outils de guerre électronique au sein des armées modernes, et il est mentionné que le terrorisme électronique a un but pour pénétrer et exploiter les plans militaires de l'État, ce qui permet d'identifier la nature de la puissance militaire de l'État et ses des tactiques militaires, et cela permet ainsi de contrôler l'affrontement des pays ciblés, que ce soit dans le domaine de la guerre conventionnelle ou dans le cyberespace.

Deuxièmement : sur le plan économique, les

cyberattaques peuvent viser l'arrêt complet d'Internet dans le pays ciblé, ce qui entraîne l'arrêt des transactions bancaires et e-gouvernement et le vol des numéros de carte de crédit et des détails qui sont achetés en ligne, ce qui entraîne la perturbation de la circulation des fonds dans le pays, et arrête ainsi Les secteurs les plus importants du pays tels que l'industrie et d'autres secteurs de l'État.

sur le plan psychologique ; Les cyberattaques peuvent viser à semer la panique dans le pays ; Comme le piratage de sites Web et la déclaration de l'état d'urgence, qui suscite l'inquiétude des citoyens et provoque une guerre psychologique.

Troisièmement : Sur le plan culturel, le terrorisme électronique peut cibler la distorsion de l'identité de l'État en promouvant les idées de l'État attaquant d'une manière qui cible la jeunesse de l'État et affecte leurs idées et croyances globales dans l'État, et cela c'est ce qu'utilisent de nombreux acteurs non internationaux Comme les organisations terroristes qui ciblent les jeunes et leur font suivre un cours contre leur État, et tout cela se fait par le biais des médias sociaux et des canaux satellites.

Quatrièmement : Au niveau politique, le terrorisme électronique peut viser à attiser les conflits au sein de l'État et à mobiliser le peuple contre l'autorité au pouvoir et les discours de haine en expliquant au peuple que de nombreux dangers entourent l'État et que l'autorité au pouvoir ne fournit pas les besoins fondamentaux du

peuple, ainsi que demander au peuple de l'État ciblé d'obtenir Sur leurs droits pillés, ce qui conduit à des manifestations populaires et peut se transformer en révolutions non pacifiques visant à saboter et détruire le pays ciblé, et tout cela est dû aux plateformes de réseaux sociaux, et cet objectif a joué son rôle dans les révolutions du printemps arabe en 2011 qui ont provoqué la chute des régimes de nombreux dirigeants de pays. En fait, il y a des pays qui n'ont pas pu se remettre de ces révolutions, ce qui en a fait des zones de concurrence entre les grands pays et a même fait des organisations terroristes de ces pays une place pour eux.

Alors, la seule force militaire n'est plus la seule menace pour les pays. D'où l'évolution du concept de sécurité, de sorte que la sécurité nationale de l'État est ne se limitant plus à la sécurité militaire, mais plutôt à une sécurité nationale politique, qui se résume dans le contenu de sécurité des données numériques et des informations électroniques relatives aux partis de l'État, en plus des informations relatives aux parlements et aux agences souveraines de l'État, qui sont toutes des informations sensibles, dont la falsification peut conduire à des guerres civiles au sein de l'État, ainsi qu'à la sécurité intellectuelle et culturelle nationale, qui représente le pic de la production intellectuelle pour tout État , car elle peut contribuer à élever ou à abaisser des aspects de la sécurité nationale de l'État, comme l'aspect physique lié à la stabilité des citoyens ou soulevant des problèmes de sécurité dans l'État.

Étant donné que le système économique et scientifique du pays a été exposé à de telles guerres, la sécurité économique nationale était nécessaire, car c'est le secteur de la sécurité le plus vulnérable aux attaques électroniques. En raison de la transformation de l'économie mondiale en une économie numérique dépendante des technologies de l'information, l'exposition de ce système à de telles attaques peut entraîner d'énormes pertes économiques et nationales, ainsi que la sécurité scientifique et de recherche nationale liée aux données et informations de recherche et les institutions scientifiques et universitaires, qui constituent une future richesse nationale contenant de nombreuses découvertes et brevets.

De nombreuses cyberattaques ont joué un rôle efficace dans la gestion des interactions sur la scène mondiale ces dernières années, notamment :

– En 2019, la Russie a été victime d'une cyberattaque qui a touché son réseau électrique, et le New York Times a rapporté que des hackers américains avaient développé des programmes malveillants capables de perturber le réseau électrique russe, ce qui a conduit à l'allocation d'importantes sommes d'argent à ces travaux, des sommes initialement destinées à lutter contre le terrorisme et les guerres américaines.

Des cybersquattes entre la Russie et l'Ukraine, où le ministère ukrainien de l'Énergie a fait l'objet d'une cyberattaque coordonnée en 2015 sur le réseau électrique ukrainien.

– La série d'attaques qui ont eu lieu depuis la Russie contre l'Ukraine en 2017 autour de la Crimée, qui ont ciblé des banques, des ministères, des journaux et des compagnies d'électricité, et même utilisé des logiciels malveillants bêta, qui ont entraîné la perturbation des systèmes d'information et la perturbation du travail des gouvernement et entreprises privées.

- Selon Microsoft, plus de la moitié des cyberattaques de l'année dernière provenaient de Russie, et selon le rapport annuel de l'entreprise sur la défense numérique, 52 % des tentatives de piratage parrainées par l'État de juillet 2019 à juin 2020 étaient d'origine russe. Tandis qu'exactement un quart venait de Russie, pendant cette période d'Iran, 12 % de Chine et les 11 % restants de Corée du Nord et d'autres pays.

- Microsoft a aussi révélé que les États-Unis ont été les plus touchés par les cyberattaques l'année dernière, suivis du Royaume-Uni, tandis que plus des deux tiers 69 % des notifications NSN envoyées par Microsoft de juillet 2019 à juin 2020 étaient destinées à des clients américains, 19 % ont été attaqués des clients au Royaume-Uni, suivis de 5 % au Canada, 4 % en Corée du Sud et 3 % en Arabie saoudite.

- L'Iran représente le deuxième source d'activité cybernétique accrue soutenue par l'État. Au cours d'une période de 30 jours entre août et septembre 2019, Microsoft a observé que des pirates basés en Iran attaquaient 241 Microsoft compte client.

- La Russie dispose d'un éventail de cyberoutils offensifs qu'elle peut utiliser contre les réseaux américains, et les attaques visent à de détruire les service ou de les « perturbatrices » .

- Les États-Unis accusent depuis longtemps la Russie de mener des attaques contre des installations américaines vitales, tandis que Washington est conscient que la capacité de la Russie à mener des cyberattaques destructrices ou destructrices peut rester très élevée.

- L'année dernière, les États-Unis ont déclaré que des cybercriminels basés en Russie avaient causé l'année dernière deux des cyberattaques les plus destructrices de mémoire récente.

Colonial Pipeline a été victime d'une attaque de ransomware en mai 2021, qui a interrompu ses opérations et provoqué des pannes généralisées dans tout le pays.

- Washington accuse également Moscou d'avoir piraté SolarWinds fin 2020, alors que les États-Unis affirment que des cybercriminels soutenus par la Russie ont eu accès à 10 agences gouvernementales américaines, dont le Département de la sécurité intérieure et le Département du commerce.

- Selon le magazine Forbes, les cyberattaques récentes des 20 dernières années contre 000 18 utilisateurs publics et privés américains dépassent les limites de l'espionnage traditionnel ; Il s'agit plutôt d'actes de cyberagression de la Russie contre les régimes américains qui durent

depuis vingt ans.

- Les attaques russes contre l'Amérique ont commencé en 1996 avec l'attaque du Moonlight Maze, l'une des premières campagnes de cyberespionnage parrainées par Moscou, selon Forbes.

- La Russie a été blâmée pour les attaques du Moonlight Maze, qui impliquaient le vol d'une quantité massive d'informations classifiées de plusieurs agences gouvernementales, dont le ministère de l'Énergie, la NASA et le ministère américain de la Défense.

- En 2008, un groupe de piratage russe appelé Turla a commencé à attaquer les systèmes militaires américains en utilisant la tromperie, les portes dérobées, les rootkits et en infectant les sites Web du gouvernement.

Dans le même temps, les services de renseignement russes ont été blâmés pour l'attaque ; Alors qu'en 2017, quatre chercheurs en informatique de Kaspersky Labs et du Kings College de Londres ont réussi à acquérir le serveur tiers utilisé pour diriger les attaques de Moonlight Maze ; Les résultats ont montré que la Russie est derrière tout cela.

Il y a plusieurs années, un autre groupe de piratage russe connu sous le nom d'APT28- a piraté le Comité national démocrate, ainsi que la Maison Blanche, les parlements allemand et norvégien, l'Organisation pour la sécurité et la coopération en Europe et des journalistes.