مجلة بحوث الإعلام الرقمي

دورية علمية محكّمة تصدر عن كلية الإعلام وتكنولوجيا الاتصال - جامعة السويس

- الحرب الرقمية
  أ.د. أمين سعيد عبد الغني
- إشـــكاليات بحـوث الإعـــلام الرقمي
  أ.د. حسن علي محمد
- الاتجاهات الحديثة في دراسات وممارسات الإعلام
  أ.د. عبد الله الرفاعي
- أثر وسائل التواصل الاجتماعي في تعزيز الهوية الوطنية لدى الشباب الكويتي
  أ. د. مناور الراجحي - د. سليمان محمد
- أخلاقيات العلاقات العامة وممارستها
  أ. د. عبدالرزاق الدليمي - أ. وليد كاطع
- توظيف الأسطورة في وسائل الإعلام
  أ. د. عبدالرزاق الدليمي
- الحرب الرقمية والأمن السيبراني
  أ. د. حبيب البدوي
- الصحافة العلمية في ضوء التأهيل الإعلامي الأكاديمي بالجامعات المصرية
  د. سهير سيف الدين - د. إيمان إبراهيم
- المداخل النظرية لدراسة الأداء المهني للقائم بالاتصال في الدراسات الإعلامية
  د. مدحت رشدي

العدد الثالث: يناير – يونيه ٢٠٢٤

مجلة بحوث الإعلام الرقمي

العدد الثالث: يناير-يونيه ٢٠٢٤

Digital Media Research Journal

Quarterly Scientific Journal issued by The Faculty of Media and Communication Technology - Suez University

- **Digital War.**
  Prof. Dr. Amin Said AbdulGhani
- **Problems of Digital Media Research.**
  Prof. Dr. Hassan Ali Muhammad
- **Modern Trends in Media Studies and Practices.**
  Prof. Dr. Abdullah Al-Rifai
- **Impact of Social Media on Enhancing National Identity among Kuwaiti Youth.**
  Prof. Dr. Manawer Al-Rajhi, Dr. Suleiman Muhammad
- **Ethics of Public Relations Practice.**
  Prof. Dr. AbdulRazzaq Al-Dulaimi, Dr. Walid Katea
- **Employing Myth in the Media.**
  Prof. Dr. AbdulRazzaq Al-Dulaimi
- **Cyber warfare and cybersecurity.**
  Prof. Dr. Habib Al-Badawi
- **Scientific Journalism in Light of Academic Media Qualification in Egyptian Universities.**
  Dr. Sohair Seif El-Din, Dr. Iman Ibrahim
- **Theoretical Approaches of studying the Professional Performance of Communicator in Media Studies.**
  Dr. Medhat Rushdi

The 3rd Issue
Jan-June
2024

مجلة بحوث الإعلام الرقمي

دورية علمية محكّمة

تصدر عن كلية الإعلام

وتكنولوجيا الاتصال

جامعة السويس

الهيئة الاستشارية:

أ. د. أحمد فاروق رضوان	الأستاذ بكلية الإعلام - جامعة الشارقة - الإمارات
أ .د. حمدى حسن	الأستاذ بكلية الإعلام - جامعة مصر الدولية
أ. د. سامى عبدالعزيز	العميد الأسبق لكلية الإعلام - جامعة القاهرة
أ. د. سامي الشريف	عميد كلية الإعلام - الجامعة الحديثة
أ. د. سهير صالح	عميد المعهد الدولي العالي للإعلام بأكاديمية الشروق
أ. د. السيد بهنسي	الأستاذ بكلية الإعلام - جامعة عين شمس
أ. د. عادل عبدالغفار	رئيس الأكاديمية الدولية للهندسة وعلوم الإعلام
أ. د. عادل فهمي	الأستاذ بكلية الإعلام - جامعة القاهرة
أ. د. عبد الرحمن محمد الشامي	الأستاذ بقسم الإعلام - كلية الآداب - جامعة قطر
أ.د. عبد الرحمن بن نامي المطيري	الأستاذ بجامعة الإمام محمد بن سعود الإسلامية - السعودية
أ.د. عبد الرزاق محمد الدليمي	الأستاذ بكلية الخوارزمي الجامعية التقنية - الأردن
أ. د. محمد شومان	عميد كلية الإعلام - الجامعة البريطانية بمصر
أ. د. محمد سعد	الأستاذ بقسم الإعلام - كلية الآداب - جامعة المنيا
أ. د. مني الحديدي	الأستاذ بكلية الإعلام - جامعة القاهرة
أ. د. هويدا مصطفي	عميد كلية الإعلام - جامعة مصر للعلوم والتكنولوجيا

مجلة بحوث الإعلام الرقمي
دورية علمية محكّمة تصدر عن
كلية الإعلام وتكنولوجيا الاتصال- جامعة السويس

المراسلات:

ترسل المراسلات باسم الأستاذ الدكتور رئيس مجلس الإدارة ورئيس التحرير - كلية الإعلام وتكنولوجيا الاتصال - جامعة السويس- السويس- مدينة السلام (١).

تليفون: 0623523774

البريد الإلكتروني: dmrjournal@media.suezuni.edu.eg

رقم الإيداع بدار الكتب المصرية: 24417 / 2023

الترقيم الدولي للنسخة المطبوعة: ISSN: 2812-5762

أهداف المجلة:

- الإسهام في تطوير المعرفة ونشرها، وذلك بنشر البحوث العلمية الأصيلة، والمراجعات العلمية في مجالات البحوث والدراسات في مجالات تخصص الإعلام الرقمى المختلفة.
- نشر البحوث العلمية المبتكرة، التي يعدّها أعضاء هيئة التدريس والهيئة المعاونة بالجامعات المصرية والعربية، والباحثون في المجالات العلمية لتخصص الاعلام الرقمى.
- توفير فرصة التقويم العلمى للبحوث من خلال إخضاع البحوث للرأي العلمي الذى يأخذ على عاتقة تقويم الجوانب العلمية والمنهجية في البحث العلمي.
- معالجة القضايا المعاصرة في إطار البحث العلمى، وتوظيفها في خدمة المجتمع، وخدمة القضايا الجوهرية التي تأسست من أجلها المجلة، وعلى رأسها التحول الرقمى.
- رصد ومتابعة اتجاهات البحث العلمى، من خلال الوقوف على النتائج العلمية للبحوث التي تصدرها المؤسسات الأكاديمية ومراكز البحوث المتخصصة.
- اهتمامات المجلة:
- تعنى المجلة بنشر:
- البحوث العلمية الرصينة في مجالات تخصص الإعلام الرقمى.
- البحوث والدراسات النقدية التي تتصل بالإصدارات في مجالات التخصص التي تعنى بها المجلة.
- البحوث والدراسات العلمية المعنية بمعالجة المشكلات المعاصرة والقضايا المستجدة في المجتمع، وخصوصًا التحول الرقمي.
- البحوث والتقارير والترجمات العلمية، وعرض الكتب الجديدة في مجال الإعلام الرقمي ومراجعتها.
- التقارير عن المؤتمرات والندوات العلمية في تخصص الإعلام الرقمي في مصر والعالم العربي والعالم.

قواعد النشر:

- أن تكون البحوث متخصصة في مسألة من المسائل التي تهتم بها المجلة.
- أن تكون البحوث متّسمة بالعمق والأصالة، بحيث يضيف كل بحث جديداً إلى المعرفة.
- أن تكون البحوث موثقة من الناحية العلمية بالمراجع والمصادر والوثائق.
- تنشر البحوث في المجلة باللغات العربية والإنجليزية والفرنسية.
- أن يقر صاحب البحث بأن بحثه عمل أصيل له وليس مشتقاً من رسالتي الماجستير والدكتوراه العائدتين له.
- ألاّ يكون البحث قد سبق نشره، ويقدم الباحث تعهداً بذلك.
- ألاّ يكون البحث مقدماً للنشر في مجلة أخرى.
- لا يجوز نشر البحث في مكان آخر بعد إقرار نشره في مجلة كلية الإعلام جامعة السويس إلاّ بعد الحصول على إذن كتابي بذلك من رئيس التحرير.
- موافقة المؤلف على نقل حقوق النشر كافة إلى المجلة، وإذا رغبت المجلة في إعادة نشر البحث فإن عليها أن تحصل على موافقة مكتوبة من صاحبه.
- أصول البحث التي تصل إلى المجلة لا تردّ سواء أنشرت أم لم تنشر.
- يُمنح الباحث نسخة واحدة من العدد المنشور فيه بحثه مع خمس مستلات منه.

متطلبات النص المقدم للنشر:

- يجب ألاّ يزيد عدد صفحات البحث عن (٣٠ صفحة) بما فيها الأشكال والصور والجداول والمراجع)بمقاس A4 / أو حوالي ٩٠٠٠ كلمة).
- يذكر اسم المؤلف وعنوانه الحالي بعد عنوان البحث مباشرة مع ذكر عنوانه، ومرتبته العلمية، وبريده الإلكتروني.
- تقدم البحوث مكتوبة بخط Arabic Simplified حجم (١٤) للنصوص في المتن، وبالخط نفسه بحجم (١٢) للهوامش في نهاية البحث، وتكون الهوامش (٢,٥ سم) من كل طرف.

- تُدرج الرسوم البيانية والأشكال التوضيحية في متن البحث، وتكون الرسوم والأشكال باللونين الأبيض والأسود وترُقم ترقيمًا متسلسلاً، وتُكتب أسماؤها والملاحظات التوضيحية في أسفلها.
- تُدرج الجداول في متن البحث وترُقم ترقيمًا متسلسلاً وتُكتب أسماؤها في أعلاها، أما الملاحظات التوضيحية فتُكتب أسفل الجدول.
- تُذكر الهوامش آخر البحث، وتُذكر بعدها مباشرة قائمة المصادر والمراجع مرتبة ترتيباً هجائياً.
- يجب أن يحتوى البحث على ملخص وافٍ بحدود (١٥٠-٢٠٠) كلمة باللغة المكتوب فيها البحث، وملخص وافٍ أيضًا بحدود (١٥٠-٢٠٠) كلمة باللغة الإنجليزية، ويُكتب الملخصان في صفحتين مستقلتين.
- يُذكر مرة واحدة في البحث المصطلح العلمى باللغة العربية وبجانبه المصطلح باللغة الإنجليزية أو الفرنسية عند وروده أول مرة، ويُكتفى بعد ذلك بكتابته باللغة العربية.

فهرس المحتويات

- الحرب الرقمية

أ. د. أمين سعيد عبدالغني ١

- إشكاليات بحوث الإعلام الرقمي

أ. د. حسن علي محمد ٢٥

- الاتجاهات الحديثة في دراسات وممارسات الإعلام: الابتكار وريادة الأعمال الإعلامية

أ. د. عبدالله بن محمد الرفاعي ٣١

- أثر وسائل التواصل الاجتماعي في تعزيز الهوية الوطنية لدى الشباب الكويتي: دراسة ميدانية

أ. د. مناور بيان الراجحي ود. سليمان محمد ٦٥

- أخلاقيات العلاقات العامة وممارستها: بحث تأصيلي تنظيري

أ. د. عبدالرزاق محمد الدليمي وأ. وليد كاطع ١٠٣

- توظيف الأسطورة في وسائل الإعلام: بحث استقرائي تحليلي في إطار القرن ٢١

أ. د. عبدالرزاق محمد الدليمي ١٢٩

- الحرب الرقمية والأمن السيبراني: خطر التهديدات يقابله تعزيز الدفاعات

أ. د. حبيب البدوي ١٥٣

- الصحافة العلمية في ضوء التأهيل الإعلامي الأكاديمي بالجامعات المصرية

د. سهير سيف الدين ود. إيمان إبراهيم ١٨١

فهرس المحتويات

- **المداخل النظرية لدراسة الأداء المهني للقائم بالاتصال في الدراسات الإعلامية**

د. مدحت رشدي ١٩٩

- **دور مواقع التواصل الاجتماعي في تنمية وعي المرأة السعودية بالأمن الغذائي**

أ. آلاء عبدالمحسن، تحت إشراف أ.م.د. سالي أسامة ٢٣٥

- **دور منصات التواصل الاجتماعي للأندية الرياضية في الحد من التعصب الرياضي**

أ. منيره عبد الرحمن، تحت إشراف أ. م. د. سالي أسامة ٢٦٧

- **تحليل مشاعر مستخدمي منصة (X) للمرأة السعودية**

أ. نوره فهيد عيد، تحت إشراف أ. م. د. سالي أسامة ٢٩٩

مقدمة العدد

"أما قبل"

إن صدور مجلة علمية متخصصة هو ميلاد أمل جديد، وخصوصًا إذا كانت هذه المجلة بعنون "مجلة بحوث الإعلام الرقمي"؛ لأنها تأخذنا مباشرة إلى ساحات علوم المستقبل، وهي علوم وبحوث العصر الرقمي الذي تعيشه الإنسانية الآن، ويأتي العدد الثالث من هذه المجلة الوليدة أيضا كخطوة من خطوات استكمال البناء العلمي لكلية الإعلام وتكنولوجيا الاتصال بجامعة السويس، وذلك بعد اعتماد وبدء برنامج الماجستير: «الإعلام الرقمي»، وهو أحد البرامج الخاصة بالدراسات العليا بالكلية، فضلا عن الدبلومات المهنية، التي تم اعتمادها أيضا، والعمل مستمر في باقي البرامج في مرحلتي الماجستير والدكتوراه للانتهاء منها قريبا إن شاء الله.

ويطالع القارئ في هذا العدد مقالين علميين، المقال الأول تحت عنوان: «الحرب الرقمية»، للأستاذ الدكتور أمين سعيد، عميد الكلية. والمقال الثاني للأستاذ الدكتور حسن علي، العميد الأسبق للكلية، وهو بعنوان: «إشكاليات بحوث الإعلام الرقمي».

كما يضم هذا العدد بين دفّتيه عشر دراسات تتناول موضوعات بحثية على قدر كبير من الأهمية، فقد جاءت الدراسة الأولى تحت عنوان: «حول الاتجاهات الحديثة في دراسات وممارسات الإعلام: الابتكار وريادة الأعمال الإعلامية»، قراءة وترجمة وتحرير الأستاذ الدكتور عبدالله بن محمد الرفاعي، الأستاذ بقسم الصحافة والإعلام الجديد، كلية الإعلام والاتصال، جامعة الإمام محمد بن سعود بالرياض.

أما الدراسة الثانية فقد أعدها كلّ من الأستاذ الدكتور مناور بيان الراجحي، الأستاذ بقسم الصحافة، كلية الآداب، جامعة الكويت، والدكتور سليمان محمد آرتي، الأستاذ المساعد بقسم النقد والأدب المسرحي وعضو مجلس إدارة المجلس الوطني للثقافة والفنون والآداب بالكويت، وهي تحت عنوان: «أثر وسائل التواصل الاجتماعي في تعزيز الهوية الوطنية لدى الشباب الكويتي: دراسة ميدانية».

وجاءت الدراسة الثالثة تحت عنوان: «أخلاقيات العلاقات العامة وممارستها: بحث تأصيلي تنظيري»، وهي من إعداد الأستاذ الدكتور عبدالرزاق محمد الدليمي، الأستاذ بقسم الإعلام بكلية الخوارزمي الجامعية التقنية الأردنية، والأستاذ وليد كاطع، بكلية الإدارة والاقتصاد، الجامعة المستنصرية، العراق.

أما الدراسة الرابعة فقد جاءت تحت عنوان: «توظيف الأسطورة في وسائل الإعلام: بحث استقرائي تحليلي في إطار القرن ٢١"، وهي أيضا من إعداد الأستاذ الدكتور عبدالرزاق محمد الدليمي، الأستاذ بقسم الإعلام بكلية الخوارزمي الجامعية التقنية الأردنية.

وقد جاءت الدراسة الخامسة تحت عنوان: «الحرب الرقمية والأمن السيبراني: خطر التهديدات يقابله

تعزيز الدفاعات"، وأعدها الأستاذ الدكتور حبيب البدوي، الأستاذ بقسم اللغة اليابانية جامعة لبنان.

أما الدراسة السادسة فقد كانت من إعداد كلّ من الدكتورة سهير سيف الدين والدكتورة إيمان إبراهيم، وهي تحت عنوان: «الصحافة العلمية في ضوء التأهيل الإعلامي الأكاديمي بالجامعات المصرية».

في حين جاءت الدراسة السابعة تحت عنوان: «المداخل النظرية لدراسة الأداء المهني للقائم بالاتصال في الدراسات الإعلامية»، للدكتور مدحت رشدي، الكاتب الصحفي بمؤسسة أخبار اليوم.

وتحت إشراف الدكتورة سالي أسامة، أستاذة الإعلام المشارك بجامعة الملك فيصل، جاءت الدراسات الثامنة والتاسعة والعاشرة، فكانت الدراسة الثامنة تحت عنوان: «دور مواقع التواصل الاجتماعي في تنمية وعي المرأة السعودية بالأمن الغذائي»، للأستاذة آلاء عبدالمحسن الشعيبي، الباحثة بجامعة الملك فيصل. والدراسة التاسعة كانت للأستاذة منيره عبد الرحمن الماجد، الباحثة بجامعة الملك فيصل، وهي تحت عنوان: «دور منصات التواصل الاجتماعي للأندية الرياضية في الحد من التعصب الرياضي». أما الدراسة العاشرة فقد كانت من إعداد الأستاذة نوره فهيد عيد الدوسري، الباحثة بجامعة الملك فيصل، وهي تحت عنوان: «تحليل مشاعر مستخدمي منصة (X) للمرأة السعودية».

والله من وراء القصد،،،

مدير التحرير

أ.م.د. السيد عبدالرحمن

الحرب الرقمية والأمن السيبراني

خطر التهديدات يقابله تعزيز الدفاعات

الأستاذ الدكتور حبيب البدوي

الأستاذ بقسم اللغة اليابانية جامعة لبنان

١. مقدمة

أ. معلومات أساسية عن الحرب الرقمية وتهديدها المتزايد

ب. تعريف الحرب السيبرانية

ج. غرض الدراسة وأهدافها

٢. ماهية الحرب الرقمية

أ. نظرة عامة على الحرب الرقمية وأنواعها

ب. الحرب الرقمية مقابل الجريمة السيبرانية

ج. أثر الحرب الرقمية وعواقبها

٣. ماهية الأمن السيبراني.

أ. تعريف وشرح الأمن السيبراني

ب. أهمية الأمن السيبراني في الحماية من التهديدات والهجمات السيبرانية

ج. تدابير أمن الفضاء الحاسوبي وأفضل التدابير الاحترازية

٤. تقنيات الحرب السيبرانية

أ. نظرة عامة على تكتيكات وتقنيات الحرب الرقمية الشائعة

ب. شرح مفصل لسلسلة القتل الإلكتروني

ج. خصائص التهديدات المستمرة المتقدمة (APTs) وخصائصها

د. دراسة حالات للهجمات السيبرانية وتأثيراتها

٥. الاستجابة الحكومية والدولية للحرب السيبرانية:

أ. نظرة عامة على استجابة الحكومة والحرب الرقمية الدولية

ب. التدابير القانونية الرامية إلى منع الحرب السيبرانية

ج. الاتفاقات الدولية والتعاون في مجال أمن الفضاء الحاسوبي

د. أمثلة على المبادرات الحكومية والدولية لمكافحة الحرب السيبرانية

٦. استجابات القطاع الخاص والمنظمات غير الربحية للحرب السيبرانية:

أ. نظرة عامة على استجابة القطاع الخاص والمنظمات غير الربحية للحرب السيبرانية

ب. تدابير الأمن السيبراني للتعاون مع القطاع الخاص

ج. تبادل المعلومات فيما بين مؤسسات القطاع الخاص

د. دور المنظمات غير الربحية في النظام البيئي العالمي للأمن السيبراني

٧. الاستنتاجات

أ. موجز للنقاط الرئيسية التي نوقشت في الدراسة

ب. نظرة مستقبلية على الحرب الرقمية والأمن السيبراني

ج. توصيات وسائل التصدي للحرب السيبرانية وتحسين الأمن السيبراني

كلمات مفتاحية: الأمن السيبراني، الحاسوب، الرقمي، الحرب، أمن المعلومات.

مستخلص

نظراً لأن العالم أصبح مترابطا بشكل متزايد، يستمر تهديد الحرب الرقمية في النمو، مما يشكل تحديات كبيرة للحكومات والمنظمات والأفراد، تكشف هذه الدراسة عن مظاهر الحرب السيبرانية، والدور الحاسم للأمن السيبراني في التخفيف من آثارها. إذ تبدأ بتقديم فهم شامل للحرب السيبرانية، وتمييزها عن الجريمة السيبرانية، وتسليط الضوء على عواقبها بعد ذلك، كما تتعمق الدراسة في أهمية تدابير الأمن السيبراني في الدفاع ضد التهديدات والهجمات السيبرانية، مع التركيز على أنجع الأساليب وأفضل الاستراتيجيات.

تبحث الدراسة في التكتيكات والتقنيات الشائعة المستخدمة في الحرب السيبرانية، مع التركيز على سلسلة القتل السيبراني وخصائص التهديدات المستمرة المتقدمة (APTs) من خلال دراسات الحالة المتعمقة، ويتم توضيح تأثير الهجمات الإلكترونية، مما يؤكد الحاجة الملحة للدفاعات الفعالة.

كما يتم استكشاف الاستجابات الحكومية والدولية للحرب السيبرانية، بما في ذلك التدابير السياسية والقانونية والاتفاقيات الدولية والمبادرات التعاونية كما تبحث الدراسة في دور القطاع الخاص والمنظمات غير الربحية في مكافحة الحرب السيبرانية، مع التأكيد على أهمية التعاون وتبادل المعلومات بين القطاعات الخاصة.

كما وأن هذه الدراسة تلخص النقاط الرئيسية التي تمت مناقشتها وتقدم توصيات لمعالجة الحرب الرقمية وتعزيز الأمن السيبراني من خلال فهم صور التهديد وتنفيذ تدابير اتخاذ المبادرات، يمكن للحكومات والمنظمات والأفراد تعزيز دفاعاتهم والتنقل في عالم الحرب الرقمية المتطور بمزيد من المرونة.

تضمنت عملية البحث الخطوات التالية:

١. جمع البيانات: تم جمع معلومات عن الأنواع المتميزة للحرب السيبرانية، وتدابير الأمن السيبراني، والتكتيكات والتقنيات الشائعة، والاستجابات الحكومية والدولية، ومبادرات القطاع الخاص والمنظمات غير الربحية، ودراسات حالة للهجمات السيبرانية من المصادر المحددة، وتم التركيز على اختيار مصادر موثوقة لضمان دقة ومصداقية المعلومات.

٢. التحليل والتوليف: تحليل البيانات التي تم جمعها بعناية، وتحديد الموضـــوعات والمفاهيم والأنماط الرئيســية، وإنشــاء روابط بين الجوانب المتميزة للحرب الســيبرانية والأمن الســيبراني لتوفير فهم شــامل للموضوع.

٣. الهيكلة والكتابة: بناء على التحليل، قسمت الدراسة إلى أقسام رئيسة وأقسام فرعية، بعد التسلسل المنطقي للأفكار، تم تجميع المعلومات، ودمج النتائج والمفاهيم ودراسات الحالة الرئيسية في الأقسام المعنية، كان الهدف هو تقديم تسلسل متماسك وشامل يدعم أهداف الدراسة.

من المهم الملاحظة بأن المنهجية لا تتضمن جمع البيانات الأولية أو البحث التجريبي فحسب، بل تعتمد أيضاً على توليف وتحليل المعرفة الحالية والأعمال العلمية لتوفير رؤى وفهم لموضوع الحرب الرقمية والأمن السيبراني.

Abstract

As the world becomes increasingly interconnected, the threat of cyber warfare continues to grow, posing significant challenges to governments, organizations, and individuals. This paper explores the evolving landscape of cyber warfare and the critical role of cybersecurity in mitigating its impact. It begins by providing a comprehensive understanding of cyber warfare, distinguishing it from cybercrime, and highlighting its consequences. Subsequently, the paper delves into the importance of cybersecurity measures in defending against cyber threats and attacks, emphasizing best practices and strategies.

The paper then examines common tactics and techniques employed in cyber warfare, focusing on the Cyberkill chain and the characteristics of advanced persistent threats (APTs). Through in-depth case studies, the impact of cyberattacks is illustrated, underscoring the urgency of effective defenses.

Government and international responses to cyber warfare are also explored, including policy and legal measures, international agreements, and cooperative initiatives. The paper further investigates the role of the private sector and non-profit organizations in combating cyber warfare, emphasizing the significance of collaboration and information sharing among private entities.

This paper summarizes the key points discussed and provides recommendations for addressing cyberwarfare and enhancing cybersecurity. By understanding the threat landscape and implementing initiative-taking measures, governments, organizations, and individuals can bolster their defenses and navigate the evolving world of cyber warfare with greater resilience.

The research process involved the following steps:

1. *Data Collection:* Information on the distinct types of cyber warfare, cyber security measures, common tactics and techniques, government and international responses, private sector and non-profit initiatives, and case

studies of cyber-attacks was collected from identified sources. The emphasis was placed on selecting reliable and authoritative sources to ensure the accuracy and credibility of the information.

2. *Analysis and Synthesis:* The collected data was carefully analyzed, and key themes, concepts, and patterns were identified. Connections between distinct aspects of cyber warfare and cybersecurity were established to provide a holistic understanding of the subject matter.
3. *Structuring and Writing:* Based on the analysis, the paper was structured into sections and subsections, following a logical flow of ideas. The information was synthesized, and key findings, concepts, and case studies were incorporated into the respective sections. The aim was to present a cohesive and comprehensive narrative that supports the objectives of the paper.

It is important to note that the methodology does not involve primary data collection or empirical research; instead, it relies on the synthesis and analysis of existing knowledge and scholarly works to provide insights and understanding of the topic of cyber warfare and cybersecurity.

ملخص تنفيذي

يستمر تهديد الحرب الرقمية في التصاعد في عالمنا المترابط، مما يستلزم فهما قويا للمشهد وتنفيذ تدابير فعالة للأمن السيبراني بحيث قدمت هذه الدراسة تحليلاً مسهباً للحرب السيبرانية وأنواعها والتمييز بين الحرب الرقمية والجريمة السيبرانية، وتم تسليط الضوء على عواقب الحرب السيبرانية، مع التأكيد على الحاجة إلى استراتيجيات دفاعية استباقية.

برز الأمن السيبراني كعنصر حاسم في الحماية من التهديدات والهجمات السيبرانية، وقد أكدت الدراسة على أهمية تدابير الأمن السيبراني وأفضل الممارسات، مع التأكيد على الحاجة إلى التكيف والتحصين المستمر في مواجهة التهديدات المتطورة.

إن تحليل تكتيكات وتقنيات الحرب الرقمية الشائعة، لا سيما سلسلة القتل السيبراني والتهديدات المستمرة المتقدمة (APTs)، سلّط الضوء على الطبيعة المعقدة للهجمات السيبرانية من خلال دراسات الحالة، إذ تم إثبات تأثير الحرب الرقمية في العالم الحقيقي، وهو بمثابة تذكير صارخ بالحاجة الملحة لتعزيز الدفاعات.

ولقد تم استكشاف الاستجابات الحكومية والدولية للحرب السيبرانية، بما في ذلك التدابير السياسية والقانونية والتعاون الدولي والمبادرات التعاونية بالإضافة إلى ذلك، تمت مناقشة دور القطاع الخاص والمنظمات غير الربحية في مكافحة الحرب السيبرانية، مع التأكيد على أهمية التعاون وتبادل المعلومات. كما تخلص الدراسة إلى أنه من الواضح أن التصدي للحرب السيبرانية يتطلب نهجا متعدد الأوجه يشمل الحكومات والمنظمات والأفراد.

تتطلب الطبيعة المتطورة للحرب السـيبرانية البحث المسـتمر والابتكار والتكيف من خلال البقاء على اطلاع متواصل على أحدث المستجدات، وتنفيذ تدابير فعالة للأمن السيبراني، وتعزيز التعاون، عندها يمكننا أن نصـل الى مشـهد رقمي أكثر أمانا ومرونة؛ ومن الأهمية بمكان أن يعمل معاً أصـحاب المصـلحة عبر مختلف القطاعات لتخفيف من التهديد المتزايد للحرب السـيبرانية وحماية سـلامة واسـتقرار بنيتنا التحتية الرقمية.

Executive Summary

The threat of cyber warfare continues to escalate in our interconnected world, necessitating a robust understanding of the landscape and the implementation of effective cybersecurity measures. This paper provides an in-depth exploration of cyber warfare, its types, and the distinction between cyber warfare and cybercrime. The consequences of cyber warfare have been highlighted, emphasizing the need for proactive defense strategies.

Cybersecurity has emerged as a critical component of safeguarding against cyber threats and attacks. The paper underscores the importance of cybersecurity measures and best practices, emphasizing the need for continuous adaptation and improvement in the face of evolving threats.

The analysis of common cyber warfare tactics and techniques, particularly the cyberkill chain and advanced persistent threats (APTs), has shed light on the intricate nature of cyberattacks. Through case studies, the real-world impact of cyber warfare has been demonstrated, serving as a stark reminder of the urgency to bolster defenses.

Government and international responses to cyberwarfare have been explored, including policy and legal measures, international cooperation, and collaborative initiatives. Additionally, the role of the private sector and non-profit organizations in combating cyberwarfare has been discussed, emphasizing the importance of collaboration and information sharing.

As the paper concludes, it is evident that addressing cyber warfare requires a multi-faceted approach involving governments, organizations, and individuals. Recommendations have been provided to guide efforts in combating cyber warfare and improving cybersecurity, including the development of robust policies and legal frameworks, international cooperation, public-private partnerships, and increased awareness and education.

The evolving nature of cyber warfare necessitates ongoing research, innovation, and adaptation. By continually staying informed, implementing effective cybersecurity measures, and fostering collaboration, we can strive towards a more secure and resilient digital landscape. It is crucial that stakeholders across sectors work together to mitigate the growing threat of cyber warfare and protect the integrity and stability of our digital infrastructure.

١. المقدمة

أ. معلومات أساسية عن الحرب الرقمية وتهديدها المتزايد

الحرب الرقمية هي استخدام الهجمات السيبرانية ضد دولة معادية، مما يتسبب في ضرر مماثل للحرب الفعلية و/ أو تعطيل أنظمة الحاسوب الحيوية، عادة ما يتم تعريفه على أنه هجوم إلكتروني أو سلسلة من الهجمات التي تستهدف دولة ما، ولدى هذه الحرب القدرة على إحداث فوضى في البنية التحتية الحكومية والمدنية وتعطيل الأنظمة الحيوية، مما يؤدي إلى إلحاق أضرار بالدولة والتسبب حتى خسائر في الأرواح. عادة ما تنطوي الحرب الرقمية على دولة قومية ترتكب هجمات إلكترونية على دولة أخرى، ولكن في بعض الحالات، يتم تنفيذ الهجمات من قبل المنظمات الإرهابية أو الجهات الفاعلة من غير الدول التي تسعى إلى تعزيز أهداف دولة معادية[١].

يمكن أن تتخذ الحرب الرقمية أشكالا عديدة، ولكن جميعها تنطوي إما على زعزعة استقرار، أو تدمير الأنظمة الحيوية للجهة المستهدفة. والهدف هو إضعاف البلد المستهدف من خلال المساس بأنظمته الأساسية.

يمكن استخدام الهجمات الإلكترونية التي تخرب أنظمة الحواسيب الحكومية لدعم الحرب التقليدية، لقد أصبحت الوظائف في الحرب الإلكترونية ذات شعبية متزايدة في الجيش، وجميع الفروع الأربعة لجيش الولايات المتحدة تجند بفعالية أشخاصاً لملئ مناصب في جهاز الحرب الإلكترونية.

ب. تعريف الحرب السيبرانية

الحرب الرقمية هي استخدام الهجمات السيبرانية ضد دولة معادية، مما يتسبب في ضرر مماثل للحرب الفعلية وتعطيل أنظمة الحاسوب الحيوية؛ التعريف المقبول للحرب السيبرانية هو سلسلة من الهجمات السيبرانية ضد دولة، مما يتسبب في ضرر كبير، والذي يمكن أن يشمل تعطيل أنظمة الحاسوب الحيوية، حتى الخسائر في الأرواح.

عادة ما تنطوي الحرب الرقمية على دولة ترتكب هجمات إلكترونية على دولة أخرى، ولكن في بعض الحالات، يتم تنفيذ الهجمات من قبل منظمات إرهابية أو جهات فاعلة من غير الدول، وتسعى إلى تعزيز أهداف دولة معادية.

تسعى الحرب الرقمية إلى تعزيز أهداف دولة على حساب دولة أخرى وتحمل القدرة على التسبب في أضرار للبنية التحتية الحكومية والمدنية، مما قد يؤدي إلى تعطيل الأنظمة الحيوية، التي تؤدي بدورها إلى إلحاق الضرر بالدولة أو الى خسائر في الأرواح[٢]. تشير الحرب الرقمية عادة إلى التقنيات المستخدمة أثناء الانخراط في الحرب السيبرانية.

ج. غرض الدراسة وأهدافها

توفر بعض نتائج البحث معلومات عن الحرب السيبرانية، وتعريفها، وأصولها، ودوافعها[٣]. الهدف هو تحديد بعض الحدود التي تحكم دمج الهجوم السيبراني الآلي كأداة للسياسة الوطنية والجماعية[٤].

٢. ماهية الحرب السيبرانية؟

أ. نظرة عامة على الحرب الرقمية وأنواعها

الحرب الرقمية هي استخدام الهجمات السيبرانية ضد دولة معادية، مما يتسبب في ضرر مماثل للحرب الفعلية وتعطيل أنظمة الحاسوب الحيوية. يمكن أن يمثل العديد من التهديدات تجاه الدولة، بما في ذلك التجسس، أو التخريب، أو الدعاية، أو التلاعب، أو الحرب الاقتصادية. ويمكن استخدام هجمات الحرب الرقمية لدعم الحرب التقليدية، مثل العبث بتشغيل الدفاعات الجوية عبر الوسائل السيبرانية من أجل تسهيل الهجوم الجوي.

هناك عدة أنواع من هجمات الحرب السيبرانية، بما في ذلك التجسس وهجمات رفض الخدمة (DoS)، وهجمات الشبكة الكهربائية، والتخريب[٥]؛ الحرب الرقمية هي سلسلة من الهجمات والهجمات المضادة بين الدول باستخدام أدوات ومنهجيات إلكترونية هجومية ودفاعية. إن الهدف من الحرب الرقمية هو الفرق الأساسي بين الحرب الرقمية والجرائم الإلكترونية الأخرى، لذا يمكن أن تتخذ الحرب الرقمية أيضا شكل نشاط من نوع العمليات الخاصة، مثل عملية Stuxnet السيبرانية ضد إيران[٦].

ب. الحرب الرقمية مقابل الجرائم السيبرانية

تختلف الحرب الرقمية والجرائم السيبرانية من حيث أهدافها والأطراف المعنية. فالحرب الرقمية هي سلسلة من الهجمات والهجمات المضادة بين الدول باستخدام أدوات ومنهجيات إلكترونية هجومية ودفاعية، في حين أن الجريمة السيبرانية هي جريمة محورها الإنسان ترتكب في بيئة رقمية[٧].

إن الفرق الوحيد الملموس بين الحرب الرقمية والجرائم السيبرانية الأخرى هو هدف المقاتلين، وربما مواردهم، غالبا ما يترافق تنفيذ الجرائم الإلكترونية بتحقيق مكاسب مالية، في حين أن الحرب الإلكترونية والإرهاب السيبراني يمكن أن يكون لهما أضرار أكبر بكثير، بما في ذلك الآلاف من الأرواح المفقودة، وإصابة الناس، وتعطيل قدرة المجتمع على الحفاظ على النظام العام[٨]. لقد أصبحت الخطوط الفاصلة بين الجريمة السيبرانية والحرب الرقمية غير واضحة بمرور الوقت، وأدت طبيعة الفضاء السيبراني إلى تعقيد النيات الموجودة مسبقا للهجمات المسلحة[٩].

ج. تأثير وعواقب الحرب السيبرانية

يمكن أن يكون للحرب السيبرانية آثار وعواقب كبيرة، بما في ذلك تعطيل أنظمة الحاسوب الحيوية، والخسائر في الأرواح، وإصابة الناس، وتعطيل قدرة المجتمع على الحفاظ على النظام. عادة ما يتم تعريف الحرب الرقمية على أنها سلسلة من الهجمات الإلكترونية ضد دولة معينة، مما يتسبب في ضرر كبير لها

يمكن أن يشمل الضرر الناجم عن الحرب الرقمية تعطيل أنظمة الحاسوب الحيوية حتى الخسائر في الأرواح يمكن أن تتخذ الحرب الرقمية أشكالا عديدة، ولكن جميعها تنطوي إما على زعزعة استقرار أو تدمير الأنظمة الحيوية[١٠].

إن الدوافع وراء الحرب الرقمية هي دوافع: عسكرية ومدنية والدخل القومي وتعزيز أهداف الدولة، فالحرب الرقمية هي امتداد للسياسة من خلال الإجراءات المتخذة في الفضاء السيبراني من قبل الجهات الفاعلة الحكومية التي تشكل تهديدا خطيرا لأمن دولة أخرى.

٣. ماهية الأمن السيبراني

أ. تعريف الأمن السيبراني

الأمن السيبراني هو ممارسة حماية الأنظمة الحيوية والمعلومات الحساسة والشبكات والأجهزة والبرامج والبيانات من الهجمات الرقمية، سواء كانت هذه التهديدات تنشأ من داخل المؤسسة أو خارجها. كما يعرف أيضا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكتروني[١١].

لقد تم تصميم تدابير الأمن السيبراني لمكافحة التهديدات ضد الأنظمة والتطبيقات الشبكية، بما في ذلك الهجمات الإلكترونية التي تحاول الوصول إلى البيانات، أو تغييرها، أو تدميرها، أو ابتزاز الأموال من المستخدمين أو المؤسسة، أو تهدف إلى تعطيل العمليات التجارية العادية[١٢].

يحتوي نهج الأمن السيبراني الناجح على طبقات متعددة من الحماية تنتشر عبر أجهزة الحاسوب، أو الشبكات، أو البرامج، أو البيانات التي ينوي المرء الحفاظ عليها آمنة[١٣]. كما يعتمد الأمن السيبراني على بروتوكولات التشفير لتشفير رسائل البريد الإلكتروني والملفات والبيانات الهامة الأخرى لحماية المعلومات أثناء النقل.

ب. أهمية الأمن السيبراني في الحماية من التهديدات والهجمات السيبرانية

للأمن السيبراني أهمية قصوى كونه يحمي الأفراد والشركات والحكومات من التهديدات والهجمات السيبرانية[١٤]. ويمكن للأمن السيبراني مراقبة الأنظمة بحثا عن السرقة ومنع خروقات البيانات، فضلا عن الجرائم الإلكترونية الأخرى[١٥].

من المهم الاستثمار في الأمن السيبراني لحماية البيانات والأصول من المجرمين، حيث إن حجم وتطور الهجمات الإلكترونية في تزايد مستمر يساعد الأمن السيبراني على تأمين الأنظمة والشبكات ضد هذه التهديدات، ويمكن أن يمنح الشركات ميزة تنافسية من خلال تحسين وضعها الأمني وجعل الأمر أكثر صعوبة على المهاجمين لاختراق أنظمتهم. ولقد أصبح ضمان وجود مواهب كافية في مجال الأمن السيبراني في الولايات المتحدة والعالم أولوية قصوى عبر القطاعات والدول[١٦].

ج. تدابير الأمن السيبراني وأفضل الممارسات

تدابير الأمن السيبراني وأفضل الممارسات ضرورية للحماية من التهديدات والهجمات السيبرانية يعد وضع سياسة قوية للأمن السيبراني دليلا رسميا لجميع التدابير المستخدمة في الشركة لتحسين كفاءة الأمن السيبراني، ويعد تعليم العادات الجيدة مثل تغيير كلمة المرور، والحصول على كلمة مرور قوية، ومصادقة ٢-factor جزءا مهما من الأمن السيبراني[١٧]

كما يعد تنفيذ أفضل ممارسات الأمن السيبراني الآمن أمرا مهما للأفراد والمؤسسات من جميع الأحجام، بما في ذلك استخدام كلمات مرور قوية وتحديث البرامج والتفكير قبل النقر على الروابط المشبوهة وتشغيل المصادقة متعددة العوامل[١٨]. لذا يعد الحفاظ على تحديث البرامج وتثبيت آخر تحديثات الأمان للأجهزة وإدراك البيانات المحمية من تدابير الأمن السيبراني المهمة أيضا[١٩]. ويجب أن تعمل جهود وأدوات قياس الأمن السيبراني على تحسين جودة المعلومات وفائدتها لدعم اتخاذ القرارات الفنية ورفيعة المستوى للمؤسسة حول أخطار الأمن السيبراني وكيفية إدارتها على أفضل وجه[٢٠].

تقنيات الحرب الرقمية

أ. نظرة عامة على تكتيكات وتقنيات الحرب الرقمية الشائعة

الحرب الرقمية هي استخدام الهجمات السيبرانية ضد دولة معادية، مما يتسبب في ضرر مماثل للحرب الفعلية وتعطيل أنظمة الحاسوب الحيوية. يمكن استخدام تكتيكات وتقنيات الحرب الرقمية لتحقيق الأهداف المستهدفة، وأحيانا بطريقة سرية تقع تحت عتبة النزاع المسلح التقليدي. ويمكن استخدام الأدوات السيبرانية في شكل عمليات تقليدية، مثل تعطيل عقد القيادة والتحكم، أو في نشاط من نوع العمليات الخاصة، مثل عملية Stuxnet السيبرانية ضد إيران. لذا تشكل الحرب الرقمية العديد من التهديدات تجاه الدولة، بما في ذلك التجسس، أو التخريب، أو الدعاية، أو التلاعب، أو الحرب الاقتصادية.

تتطلب الحرب الرقمية تعاون العديد من الأفراد من مختلف المنظمات والوحدات الحكومية، ويمكن أن تجمع الألعاب الحربية الإلكترونية هؤلاء الأشخاص لمساعدتهم على تحديد كيفية العمل معا في حالة وقوع هجوم إلكتروني. وللحماية من الحرب السيبرانية، يجب على المنظمات والأفراد تنفيذ أفضل ممارسات الأمن السيبراني، مثل وضع سياسة قوية للأمن السيبراني، واستخدام كلمات مرور قوية، وتحديث البرامج، وتشغيل مصادقة متعددة العوامل[٢١].

ب. سلسلة القتل السيبراني Chain Cyber Kill

إن الاطلاع على "سلسلة القتل السيبراني" هو ضرورة ملحة لوضع خطط الأمن السيبراني، فهو يصف مراحل الهجوم السيبراني ويساعد المؤسسات على فهم تسلسل الأحداث التي ينطوي عليها هجوم خارجي على

بيئة تكنولوجيا المعلومات الخاصـــة بها[٢٢]، إطار عمل Chain Cyber Kill، الذي طورته شـــركة لوكهيد مارتن، يشرح كيفية تنقل المهاجمين عبر الشبكات لتحديد نقاط الضعف التي يمكنهم استغلالها بعد ذلك[٢٣].

سلسلة القتل السيبراني هي نهج خطوة بخطوة يحدد ويوقف نشاط العدو، ويحدد المراحل المختلفة للعديد من الهجمات الإلكترونية الشائعة[٢٤]، وتشمل مراحل سلسلة القتل السيبراني تحديد الهدف والإرسال والقرار والأمر وتدمير الهدف[٢٥].

يمكن أن يســـاعد فهم نموذج Cyber Kill Chain على إحداث فرق في أمن تكنولوجيا المعلومات، وعلى وضع استراتيجيات وتقنيات "لقتل" أو احتواء الهجوم في مراحل مختلفة[٢٦]. تسمح سلسلة القتل السيبراني لفريق أمن المعلومات بإعاقة الهجوم خلال مرحلة معينة، ثم تصميم تدابير أقوى للأمن السيبراني.

ج. مراحلها التهديدات المستمرة المتقدمة (APTs) وخصائصها

التهديدات المستمرة المتقدمة (APTs) هي نوع من الهجمات الإلكترونية المصممة خصيصا للوصول غير المسموح به إلى المعلومات أو الأنظمة أو الشبكات الحساسة. وعادة ما يتم إجراء (APTs) بواسطة مهاجمين يتمتعون بمهارات عالية، ولديهم الكثير من الموارد، ويعرفون اهدافهم، وهم دائماً مســـتمرون في جهودهم للتسلل إلى الشبكة المستهدفة. ويمكن تقسيم هجوم APT الناجح إلى ثلاث مراحل: التسلل إلى الشبكة، توسيع وجود المهاجم، واستخراج البيانات المتراكمة، كل ذلك دون أن يتم اكتشافه[٢٧].

غالبا ما تستخدم (APTs) تكتيكات الهندسة الاجتماعية أو تستغل نقاط ضعف البرامج في المؤسسات ذات المعلومات عالية القيمة[٢٨]. وهناك العديد من الخصائص التي تميز هجمات الأمن السيبراني APT عن غيرها، بما في ذلك طبيعتها المتقدمة، وارتفاع تكاليف التخصيص، ومشاركة فريق من مجرمي الإنترنت ذوي المهارات العالية والذكاء[٢٩]. كما أن هناك أنواع مختلفة من (APTs)، بما في ذلك (APTs) التي ترعاها الدولة، و(APTs) لمجرمي الإنترنت، و(APTs) المتسللين، ولكل منها أهدافها ودوافعها الخاصـــة. لذا يعد فهم خصائص وأنواع (APTs) أمرا مهما للمؤسسات للدفاع بشكل أفضل ضد هذه الأنواع من الهجمات[٣٠].

د. دراسات حالة للهجمات الإلكترونية وتأثيرها.

إن التهديدات المســتمرة المتقدمة (APTs) هي هجمات إلكترونية ســرية على شــبكة الحاســوب، حيث يكسب المهاجم ويحافظ على وصول غير مسموح به إلى الشبكة المستهدفة، ويظل غير مكتشف لفترة طويلة. وتتميز (APTs) بالتخفي والمثابرة، والاستهداف المحدد، والهجمات متعددة المراحل، والتخطيط طويل المدى، والتقنيات المتطورة. كما تعتبر (APTs) متقدمة ويمكن أن تكلف آلاف إلى ملايين الدولارات لتخصــيصــها، مما يتطلب فريقا من مجرمي الإنترنت ذوي المهارات العالية والذكاء لإنشـائها. لذا فإن الهدف الأسـاسـي من

(APTs) هو سرقة البيانات، ولكن هناك أدلة متزايدة على أهداف أخرى مثل برامج الفدية والتجسس وتعطيل الأنظمة وتعدين العملات المشفرة[٣١].

٤. الاستجابة الحكومية والدولية للحرب السيبرانية

أ- نظرة عامة على استجابة الحكومة والحرب الرقمية الدولية

إن الحاجـــة إلى التعاون الدولي بين الدول والمنظمات الدولية والإقليمية والكيانات الأخرى، يعد أمرا بالغ الأهمية في إدارة الحروب الإلكترونية والهجمات السـيبرانية. تحتاج الحكومات إلى ضـمان حماية بنيتها الالكترونية التحتية بشـكل جيد ضـد أنواع مختلفة من التهديدات السـيبرانية، وأن أطرها القانونية والسـياسـية تسمح لها بمنع الهجمات الإلكترونية المحتملة وردعها والدفاع عنها والتخفيف من حدتها بشكل فعال.

على الرغم من عدم وجود توافق في الآراء حول ما يشكل بالضبط الحرب الرقمية أو الإرهاب السيبراني، قد تصـبح مجالات مثل تبادل المعلومات والاسـتخبارات والمسـاعدة المتبادلة ضـرورية في الاسـتجابة للأزمة السيبرانية.

إن التعريف المقبول عموما للحرب السيبرانية هو سلسلة من الهجمات الإلكترونية ضد دولة معينة، مما تسـبب لها في ضـرر كبير. تسـعى الحرب الرقمية إلى تعزيز أهداف دولة على حسـاب دولة أخرى، وتحمل القدرة على التســبب في أضــرار للبنية التحتية الحكومية والمدنية، مما قد يؤدي إلى تعطيل الأنظمة الحيوية التي تفضـــي بدورها إلى الضـــرر والتهديد للأمن القومي للدولة. كما لا تريد الحكومات تزويد الأعداء برؤى حول سـياسـات الدفاع السـيبراني الخاصـة بهم، ولا تريد أن تكون دقيقة للغاية بشـأن الاسـتجابات المحتملة للهجمات الإلكترونية لمنع وضـــع خطوط حمراء، إذا تم تجاوزها، قد تلزمهم بالتصـــرف بنتيجة غير مرغوب فيها[٣٢].

ب – التدابير القانونية الرامية إلى منع الحرب السيبرانية

لقد اعترفت الحكومات والمنظمات الدولية بالحاجة إلى تدابير ســـياســـية وقانونية لمنع الحرب الرقمية والتهديدات السـيبرانية. تحتاج الحكومات إلى ضـمان حماية بنيتها التحتية بشـكل جيد ضـد أنواع مختلفة من التهديدات السـيبرانية وأن أطرها القانونية والسـياسـية سـتسـمح لها بمنع الهجمات السـيبرانية المحتملة وردعها والدفاع عنها والتخفيف من حدتها بشـكل فعال. كما أن النظام التنظيمي الذي يحكم كيفية انخراط البلدان في النشـاط السـيبراني، الهجومي والدفاعي على حد سـواء، هو أيضـا جانب مهم من التدابير السـياسـية والقانونية لمنع الحرب السيبرانية[٣٣].

ومن المهم الاتفاق على موقف مشـــترك حتى في المســـائل المتعلقة بالقواعد الراســـخة للقانون الدولي العرفي، مثل حظر اســـتخدام القوة المقنن في ميثاق الأمم المتحدة، المادة ٢ (٤)، إلى جانب الاســـتثناءين

المتمثلين في الدفاع عن النفس وقرار من مجلس الأمن[٣٤]. من هنا يعد التواصل والتعاون بين المسؤولين الحكوميين ومالكي البنية التحتية الحيوية في القطاع الخاص أمرا ضروريا لأن الجيش أكثر دراية وأفضل استعدادا للرد على أي هجوم إلكتروني[٣٥].

ج. الاتفاقات الدولية والتعاون في مجال أمن الفضاء الحاسوبي

إن الاتفاقات والتعاون الدولي ضروري في مواجهة تحديات الأمن السيبراني استناداً إلى:

- تركيز التعاون على الشراكة بين الوكالات، والشراكة بين القطاعين العام والخاص، وشبكات تبادل المعلومات، واتفاقيات التعاون[٣٦].
- تطوير اتفاقيات دولية لتبادل معلومات الأمن السيبراني لتشمل الاستجابات المشتركة للتهديدات، والتعاون في حماية البنية التحتية الحيوية.
- تحتاج الحكومات إلى ضمان حماية بنيتها التحتية بشكل جيد ضد أنواع مختلفة من التهديدات السيبرانية وأن أطرها القانونية والسياسية ستسمح لها بمنع الهجمات السيبرانية المحتملة وردعها والدفاع عنها والتخفيف من حدتها بشكل فعال.
- قد تصبح مجالات مثل تبادل المعلومات والاستخبارات والمساعدة المتبادلة ضرورية في الاستجابة للأزمة السيبرانية، ولكن فعالية اتفاقيات التعاون هذه التي من شأنها أن تعالج السلوك في الفضاء السيبراني بشكل مباشر.
- يمكن للاتفاقيات الدولية تحسين الأمن السيبراني من خلال تحديد الأنشطة التي من المحتمل أن تكون موضوعا لمثل هذه الاتفاقيات وتلك التي ليست كذلك، والتدابير التي من المحتمل أن تستخدمها الأطراف لتحسين الأمن السيبراني في كل مجال من مجالات النشاط المناسبة للأنشطة المحددة، بما في ذلك الحالات التي استخدم فيها المجرمون المزعومون الإنترنت.

د. أمثلة على المبادرات الحكومية والدولية لمكافحة الحرب السيبرانية

- هناك العديد من المبادرات الحكومية والدولية لمكافحة الحرب الرقمية، وتحتاج الحكومات إلى ضمان حماية بنيتها التحتية بشكل جيد ضد أنواع مختلفة من التهديدات السيبرانية وأن أطرها القانونية والسياسية تسمح لها بمنع الهجمات السيبرانية المحتملة وردعها والدفاع عنها والتخفيف من حدتها بشكل فعال.
- طورت الولايات المتحدة نظاما تنظيميا يحكم كيفية الانخراط في النشاط السيبراني، الهجومي والدفاعي على حد سواء، مع التركيز على الاستراتيجيات الأمريكية الناشئة، بما في ذلك "الدفاع إلى الأمام"[٣٧].
- يمكن للحكومات استخدام أدوات السياسة الخارجية مثل التحذيرات الدبلوماسية والعقوبات الاقتصادية للضغط على خصم مشتبه به وطلب المساعدة من دول أخرى.

- التعاون الدولي بين الدول والمنظمات الدولية والإقليمية والكيانات الأخرى ضـــروري لمواجهة تحديات الأمن السيبراني.
- أصـــبح الجيش أكثر انخراطاً في التصـــدي للتهديد الوطني والعالمي الذي يفرضـــه اســـتخدام المجال السيبراني، والتجنيد النشط في جميع الفروع الأربعة لجيش الولايات المتحدة لمواقع الحرب الإلكترونية.

٦. استجابات القطاع الخاص والمنظمات الغير ربحية للحرب السيبرانية

أ. نظرة عامة على استجابة القطاع الخاص والمنظمات الغير ربحية للحرب السيبرانية

اســـتجاب القطاع الخاص والمنظمات الغير ربحية للحرب الســـيبرانية من خلال تحســـين اســـتعداداتها للاســـتجابة للحوادث الســـيبرانية[٣٨]. وعادة ما تنطوي الحرب الرقمية على دولة معينة ترتكب هجمات إلكترونية على دولة أخرى، ولكن في بعض الحالات، يتم تنفيذ الهجمات من قبل منظمات إرهابية أو جهات فاعلة غير حكومية تسعى إلى تعزيز هدف دولة معادية. لذا يناقش خبراء الأمن السيبراني نوع النشاط الذي يشكل حربا إلكترونية، ولا يوجد تعريف رسمي عالمي للحرب السيبرانية.

إن إدماج الهجمات السـيبرانية الآلية كأداة للسـياسـة في الأمن الوطني والجماعي هو قضـية وتحد يجب معالجته. إن هدف المقاتلين وربما مواردهم هو الفرق الوحيد الملموس بين الحرب الرقمية والجرائم الســـيبرانية الأخرى. إن أسـلحة وحجم الحرب الرقمية متشـابهان إلى حد كبير مع الجريمة السـيبرانية، ولا توجد أسـلحة إلكترونية مخصصة فقط لصراع الدولة القومية[٣٩].

ب. تدابير الأمن السيبراني للتعاون مع القطاع الخاص

يمكن للقطاع الخاص التعاون مع الحكومة لتحســـين تدابير الأمن الســـيبراني، وتعد الشـــراكة بين القطاعين العام والخاص ضـرورية في الأمن السـيبراني الوطني، ويقوم صـانعو السـياسـات والقطاع الخاص بوضـع تصـور لدور كل منهم في الأمن السـيبراني الوطني تركز ركيزة التعاون على الشـراكة بين الوكالات والشراكة بين القطاعين العام والخاص، وشبكات تبادل المعلومات، واتفاقيات التعاون[٤٠].

ويمكن تحســين شــراكة الأمن الســيبراني بين القطاع الخاص والحكومة من خلال تطوير علوم القياس والمعايير والتكنولوجيا[٤١]. كما يجب أن تعمل جهود وأدوات قياس الأمن الســـيبراني على تحســـين جودة المعلومات وفائدتها لدعم اتخاذ القرارات الفنية ورفيعة المستوى للمؤسسة حول أخطار الأمن السيبراني وكيفية إدارتها على أفضل وجه.

يحدد البرنامج العالمي للأمن الســـيبراني للاتحاد خمس ركائز اســـتراتيجية: القانونية والتقنية والتنظيمية وبناء القدرات والتعاون، وتشـمل الركيزة التنظيمية الهياكل والسـياسـات التنظيمية بشـأن الأمن السـيبراني والوكالات المسؤولة عن تنسـيق سـياسـة الأمن السـيبراني. ولوضـع اسـتراتيجية وطنية شـاملة وفعالة للأمن

السيبراني، يقدم دليل الاتحاد لعام ٢٠١٨ بشأن تطوير أمن سيبراني وطني إرشادات بشأن وضع إطار وطني للأمن السيبراني.

ج. تبادل المعلومات بين منظمات القطاع الخاص

يعد تبادل المعلومات بين مؤسسات القطاع الخاص أمرا بالغ الأهمية لتحسين الأمن السيبراني، بحيث تسمح برامج تبادل المعلومات للحكومة بمشاركة المعلومات مع المنظمات التي تدير البنية التحتية الحيوية. ويحدد البرنامج العالمي للأمن السيبراني للاتحاد خمس ركائز استراتيجية: القانونية والتقنية والتنظيمية وبناء القدرات والتعاون، وتشمل الركيزة التنظيمية الهياكل والسياسات التنظيمية بشأن الأمن السيبراني والوكالات المسؤولة عن تنسيق سياسة الأمن السيبراني.

كما عززت حكومة الولايات المتحدة الأمن السيبراني في القطاع الخاص من خلال توفير معلومات التهديدات الحيوية والتحرك نحو التعاون الحقيقي بين القطاعين العام والخاص. وتلعب المنظمات المشاركة في تبادل المعلومات المتعلقة بمخاطر وحوادث الأمن السيبراني دورا لا يقدر بثمن في الجهد الجماعي لتحسين الأمن السيبراني. كما يمكن للشركات رفع أرضية الأمن السيبراني من خلال مشاركة الأساليب والموارد الحالية، ولا يقتصر الانخراط في مشاركة المعلومات على العلاقة بين الحكومة والشركات الفردية.

د. دور المنظمات الغير ربحية في النظام البيئي العالمي للأمن السيبراني

تلعب المنظمات غير الربحية دورا مهما في النظام البيئي العالمي للأمن السيبراني غالبا ما تقوم المنظمات غير الربحية بجمع وتخزين معلومات حساسة عن الأفراد الذين غالبا ما يكونون عرضة للخطر والمعرضين للخطر، مما يجعل بياناتهم هدفا رئيسيا لمجرمي الإنترنت. وتحتاج المنظمات غير الربحية إلى الامتثال لمعايير معينة للعمل، وتساعد معايير الأمن السيبراني في الحفاظ على الامتثال[٤٢].

تقدم المنظمات غير الربحية خدمات أساسية لمجتمعاتها، وفي حالة وقوع هجوم إلكتروني يكشف البيانات الشخصية للعملاء، تكون العواقب مهمة بشكل خاص. كما تواجه المنظمات غير الربحية عدة أنواع من المخاطر المتعلقة بالأمن السيبراني، والتي يمكن أن تؤثر بشكل مباشر على قدرة المنظمة على خدمة مهمتها وقد تعرضها أيضا لعقوبات مدنية أو جنائية[٤٣]. فيما يركز محور التعاون على الشراكة بين الوكالات والشراكة بين القطاعين العام والخاص، وشبكات تبادل المعلومات، والاتفاقيات التعاونية، وتشمل الركيزة التنظيمية الهياكل التنظيمية والسياسات المتعلقة بالأمن السيبراني والوكالات المسؤولة عن تنسيق سياسة الأمن السيبراني.

تجد المنظمات غير الربحية المشاركة في العمل الإنساني الحيوي نفسها في مواجهة أخطار متزايدة للأمن السيبراني في بيئة صعبة بالفعل[٤٤]. ويمكن للشركات رفع أرضية الأمن السيبراني من خلال مشاركة الأساليب والموارد الحالية، ولا يقتصر الانخراط في مشاركة المعلومات على العلاقة بين الحكومة والشركات الفردية[٤٥].

الاستنتاجات

أ. ملخص للنقاط الرئيسية التي نوقشت في الدراسة

إن النقاط الرئيسية التي تمت مناقشتها في الدراسة هي أهمية التعاون بين القطاعين العام والخاص للأمن السيبراني، والحاجة إلى تبادل المعلومات وتحليلها، ودور المنظمات غير الربحية في النظام البيئي العالمي للأمن السيبراني، وضرورة التعاون الدولي بشأن مسائل الأمن السيبراني الشراكة بين القطاعين العام والخاص ضرورية في الأمن السيبراني الوطني، وتركز ركيزة التعاون على الشراكة بين الوكالات والقطاعين العام والخاص، شبكات تبادل المعلومات واتفاقات التعاون.

برامج تبادل المعلومات للحكومة، تسمح بمشاركة المعلومات مع المنظمات التي تدير البنية التحتية الحيوية، ويمكن للشركات رفع أرضية الأمن السيبراني من خلال مشاركة الأساليب والموارد الحالية[٤٦]. تقوم المنظمات غير الربحية بجمع وتخزين معلومات حساسة عن الأفراد الذين غالبا ما يكونون عرضة للخطر والمعرضين للخطر، مما يجعل بياناتهم هدفا رئيسيا لمجرمي الإنترنت، كما أن الأمن السيبراني لهذه المنظمات أمر بالغ الأهمية[٤٧] . ويهدف التعاون الدولي إلى تعزيز الثقة والأمن في مجتمع المعلومات، البرنامج العالمي للأمن السيبراني للاتحاد يحدد خمس ركائز استراتيجية: القانونية، والتقنية، والتنظيمية، وبناء القدرات، والتعاون.

ب. نظرة مستقبلية على الحرب الرقمية والأمن السيبراني

إن النظرة المستقبلية للحرب السيبرانية والأمن السيبراني معقدة ومتعددة الأوجه، اذ ان الحرب الرقمية هي استخدام الهجمات الإلكترونية ضد دولة معادية، مما يتسبب في ضرر مماثل للحرب الفعلية وتعطيل أنظمة الحواسيب الحيوية. ويمكن أن تشكل الحرب الرقمية العديد من التهديدات تجاه الدولة، كذلك يمكن استخدام الهجمات الإلكترونية لدعم الحرب التقليدية. لقد توسعت تهديدات الأمن السيبراني في السنوات الأخيرة، مع هجمات برامج الفدية الضخمة والحرب الإلكترونية المفتوحة[٤٨]. من هنا يناقش خبراء الأمن السيبراني نوع النشاط الذي يشكل حربا إلكترونية، ولا يوجد بعد تعريف رسمي عالمي للحرب السيبرانية.

لقد أصبحت الوظائف في الحرب الرقمية ذات شعبية متزايدة في الجيش، وتجند جميع الفروع الأربعة لجيش الولايات المتحدة بنشاط لشغل مناصب في أجهزة الحرب السيبرانية. إن الأمن السيبراني أمر بالغ الأهمية للأمن القومي، والسؤال الأكبر في الأمن السيبراني للمستقبل، هو كيفية منع الحرب الرقمية والتقليل من تأثيراتها السلبية على الأفراد والشركات.

ج. توصيات للتصدي للحرب السيبرانية وتحسين الأمن السيبراني.

في سبيل مواجهة الحروب الرقمية، وتطوير الأمن السيبراني، نوصي بوضع سياسة قوية للأمن السيبراني، واتباع طرق جديدة لحماية سلاسل التوريد، وتطوير الأساليب الحالية لإدارة أخطار سلسلة التوريد السيبرانية، وتلبية مبادئ انعدام الثقة بحلول نهاية السنة المالية ٢٠٢٤[٤٩]. وتحتاج الحكومات إلى ضمان حماية بنيتها التحتية بشكل جيد ضد أنواع مختلفة من التهديدات السيبرانية وأطرها القانونية والسياسية، لتسمح لها بمنع الهجمات السيبرانية المحتملة وردعها والدفاع عنها والتخفيف من قوتها بشكل فعال.

إن التعاون الدولي بين الدول والمنظمات الدولية والإقليمية والكيانات الأخرى ضروري في سياق الأمن السيبراني. و من المتوقع أن يتبع المتخصصون في الأمن السيبراني طرقا جديدة لحماية سلاسل التوريد وتطوير الأساليب الحالية لإدارة أخطار سلسلة التوريد السيبرانية.

تتطور الدفاعات السيبرانية لإحباط التهديدات السيبرانية، ويمكن للاستطلاع كخدمة أن يخدم مخططات الهجوم لتشمل المخطط الأمني للمؤسسة، وموظفي الأمن السيبراني الرئيسيين، وعدد الحواسيب الخوادم (Servers)، ونقاط الضعف الخارجية المعروفة، وحتى بيانات الاعتماد المخترقة للبيع، لمساعدة مجرمي الإنترنت. يمكن للحكومات تحسين تدابير الأمن السيبراني الخاصة بها من خلال اعتماد معايير حديثة تتضمن المصادقة المتعددة العوامل (MFA)، لمنع الهجمات المستندة إلى كلمات المرور، وحماية البيانات والأنظمة الهامة بشكل أفضل[٥٠]. لذا ينبغي للحكومات أن تركز على نهج قائم على المبادئ لسياسة التوثيق لا يصف أي تكنولوجيا أو حل بمفرده ولكنه يركز على المعايير والنتائج.

يعد وضع سياسة قوية للأمن السيبراني، بمثابة دليل رسمي لجميع التدابير المستخدمة في الشركة لتحسين كفاءة الأمن السيبراني. لذا يجب على الحكومات توظيف جميع الموارد والأجهزة ذات الصلة، لتحقيق أقصى قدر من الكشف المبكر عن نقاط الضعف والحوادث المتعلقة بالأمن السيبراني على شبكاتها[٥١]. كما يجب أن تعمل جهود وأدوات قياس الأمن السيبراني على تحسين جودة المعلومات وفائدتها لدعم اتخاذ القرارات الفنية ورفيعة المستوى للمؤسسة حول أخطار الأمن السيبراني وكيفية إدارتها على أفضل وجه.

إن عواقب عدم تحسين تدابير الأمن السيبراني في الوكالات الحكومية، قد تكون كارثية، بما في ذلك تلك المتعلقة بالأمن القومي ونزاهة الانتخابات[٥٢] ونتائجها. فالأمن السيبراني هو التهديد الأول للأمن القومي الذي تواجهه البلاد، ولا ينبغي التعامل معه باستخفاف شديد؛ أي هجوم على البنية التحتية الرقمية الحيوية في قطاع واحد من البلد، يمكن أن يؤدي أيضاً إلى تعطيل في قطاعات أساسية أخرى. ففي حال لم تتمكن الحكومة من توفير اتصال رقمي آمن وموثوق به، فلن تتمكن المجتمعات من الازدهار، ولن تزدهر الاقتصادات.

يمكن أن تؤثر أخطار الأمن السيبراني على المواطنين والشركات والبنية التحتية الرقمية الحيوية. فبدون مساعدة من المواطنين والمهنيين ومنظمات القطاع الخاص، لن يكون لدى الحكومة وحدها الطاقات والموارد اللازمة لتحسين الأمن السيبراني الشامل لبلدها بأكمله[٥٣].

إن الواقع الجديد هو أن المنظمات الكبيرة تمثّل أهدافاً للإرهاب السيبراني، والشركات تعرف الخطوات اللازمة لتحسين تدابير الأمن السيبراني الخاصة بها[٥٤]. ويمكن أن يؤثر نقص تدابير الأمن السيبراني في الوكالات الحكومية على الأمن القومي للدولة بعدة طرق، ويمكن أن يؤدي أي هجوم على البنية الرقمية التحتية الحيوية في قطاع واحد من البلد إلى تعطيل في قطاعات أخرى أيضا.

إن الأمن السيبراني هو التهديد الأول للأمن القومي الذي تواجهه البلاد، ولا ينبغي التعامل معه باستخفاف شديد، وقد تكون عواقب الانتهاك، بما في ذلك تلك المتعلقة بالأمن القومي ونزاهة الانتخابات، كارثية. وتتطلب حماية الدولة من الجهات الفاعلة السيبرانية الخبيثة قواعد اللعبة، ويجب على الحكومة الفيدرالية اعتماد أفضل الممارسات الأمنية للكشف عن الحوادث السيبرانية التي تؤثر على أنظمة الأمن القومي والاستجابة لها.

لقد أصبحت الوكالات الحكومية أهدافا متزايدة للتهديدات السيبرانية، حيث يحاول المجرمون سرقة البيانات الحساسة أو التلاعب بها. ويعد وجود خطة قوية لإدارة أخطار الأمن السيبراني أمرا بالغ الأهمية لمساعدة الوكالات الحكومية على تقليل التعرض للتهديدات.

إن الحرب الرقمية هي استخدام الهجمات السيبرانية ضد دولة معادية، مما يتسبب في ضرر مماثل للحرب الفعلية وتعطيل أنظمة الحواسيب الحيوية. ويمكن أن تشكل الحرب الرقمية العديد من التهديدات تجاه الدولة، بما في ذلك التجسس، أو التخريب، أو الدعاية، أو التلاعب، أو الحرب الاقتصادية عليها.

عادة ما تنطوي الحرب الرقمية على دولة قومية ترتكب هجمات إلكترونية على دولة أخرى، ولكن في بعض الحالات، يتم تنفيذ الهجمات من قبل منظمات إرهابية أو جهات فاعلة غير حكومية تسعى إلى تعزيز هدف دولة معادية.

إن الحرب الرقمية لديها القدرة على إحداث فوضى في البنية التحتية الحكومية والمدنية وتعطيل الأنظمة الرقمية الحيوية، والتي أصبحت العامود الفقري لكل أجهزة الدولة، مما يؤدي إلى أضرار للدولة وحتى خسائر في الأرواح. ولتعزيز الدفاعات ضد الحرب السيبرانية، من المهم الفهم العميق للتكتيكات المتبعة، والحصول على رؤية أوسع في كافة مجالات التهديد[٥٥].

إن الأمن السيبراني هو قضية حاسمة تحتاج الحكومات إلى معالجتها لحماية أمنها القومي ومصالحها الاقتصادية، والحرب الرقمية هي استخدام الهجمات الإلكترونية ضد دولة معادية، مما يتسبب في ضرر مماثل لأضرار الحرب الفعلية، وتعطيل أنظمة الحواسيب الحيوية وبنيتها التحتية.

يمكن أن تشكل الحرب الرقمية العديد من التهديدات تجاه الدولة، بما في ذلك التجسس، أو التخريب، أو الدعاية، أو التلاعب، أو الحرب الاقتصادية. لقد أصبحت الوكالات الحكومية أهدافا متزايدة للتهديدات السيبرانية حيث يحاول المجرمون سرقة البيانات الحساسة أو التلاعب بها. ولمكافحة أخطار الأمن السيبراني المتزايدة، وضعت أكثر من ١٠٠ حكومة استراتيجيات دفاعية وطنية للأمن السيبراني. لذا يجب على الحكومات الاتحادية اعتماد أفضل الممارسات الأمنية وتحسين الكشف عن نقاط الضعف والحوادث الأمنية السيبرانية على شبكاتها.

إن وجود خطة قوية لإدارة أخطار الأمن السيبراني، يعد أمرا بالغ الأهمية لمساعدة الوكالات الحكومية على تقليل التعرض للتهديدات. لذا يجب أن يكون يمثل الأمن السيبراني أولوية في أعلى مستويات الأجهزة الحكومية لأي دولة. إن الاستعانة بخبرات الجهات الخارجية، يمكن أن تساعد أيضا في تحسين تدابير الأمن السيبراني.

الملاحظات الختامية

لقد جاء في تقرر الاتحاد الدولي للاتصالات (ITU) ٢٠١٠ بشأن الأبعاد الاجتماعية للأمن السيبراني أن الثورة الرقمية غيرت كيفية التعامل التجاري، وكيفية عمل الحكومات. فقد أدت العولمة والتقدم التكنولوجي إلى إضعاف البنية التحتية وبالتالي جعلتها هدفا محتملا لهجمات إرهابية، حيث تواجه البلدان أخطاراً حقيقية؛ مما سمح للأعداء أن يستغلوا مواطن الضعف التي تعاني منها أنظمة المعلومات الدقيقة. فهم يسعون الى تعطيل البنية التحتية والموارد الأساسية من أجل تهديد الأمن القومي. وهنا تكمن المخاطر الاجتماعية التي يمكن تفسيرها في ضوء الآتي:

مع الاعتماد المتزايد في الحياة اليومية، على الأنظمة المعلوماتية، والأجهزة المتصلة بالشبكة الدولية للمعلومات، وتشعب طبيعة هذه الأجهزة من هواتف خليوية، وأجهزة حوسبة شخصية، يزداد عدد المتصلين بالفضاء السيبراني، وتزداد احتمالات الاعتداءات والجريمة. وتسهل سبل التجسس الاقتصادي وتؤثر على عمليات الحكومة مثل الفيروسات وهجمات منع الخدمة وسرقة البيانات والرسائل الاقتحامية والتدليس، كلها تقوض مصداقية تكنولوجيا المعلومات والاتصالات وقدرة المجتمعات على العمل. وقد أشار تقرير صادر عن مؤسسة ماكينزى، إلى توقيع زيادة المعلومات الرقمية بمعدل ٤٤٪، خلال الأعوام الممتدة من ٢٠٠٩ إلى ٢٠٢٠.

كذلك من أبرز التهديدات السيبرانية المحتمل تزايدها في السنوات القادمة، هجوم الفدية (ransom-war)، الذي وصفته وزارة العدل الأميركية بأنه نموذج عمل جديد للجريمة السيبرانية. ويقدر مكتب التحقيقات الفيدرالي الأميركي أن المبلغ الإجمالي من مدفوعات الفدية يقترب من مليار دولار سنويا، حيث كان من المتوقع أن الشركات التجارية سوف تقع ضحية لهجوم فدية كل ١٤ ثانية بحلول ٢٠١٩. وتشير التقارير الدولية إلى أن فيروس الفدية تسبب بخسائر مالية تفوق الخمسة مليارات دولار أثناء عام ٢٠١٧، وهو معدل مرتفع جدا خلال عام واحد.

ومن أشهر الاختراقات، ما حدث من سرقة حسابات شركة ياهو حيث بلغ عدد الحسابات المسروقة ثلاث مليارات حساب، وكذلك اختراق اكيفاكس في عام ٢٠١٧، حيث تأثر ٥١٤٥ عميلاً، وذلك يتطلب بشكل ملح إفساح المجال وبشدة للأمن السيبراني تقنيا وتشريعيا وتنظيميا ونشر ثقافة المواطنة الرقمية لزيادة سلامة التعامل السيبراني.

إن التهديدات الأمنية قد ازدادت بطرق متسارعة لم يشهدها العالم من قبل حتى شملت السياحة والتجارة والاقتصاد، وطالت أمن الدول والمجتمعات .وفي هذا الصدد، أشار تقرير صادر عن وكالة الأمن القومي الأمريكي إلى أن هناك ٢٣٢ جهاز حاسب آلي يتعرض لاختراقات وهجمات سيبرانية فى كل دقيقة على امتداد العالم مما أضاف صعوبة عالية فى المقدرة على اللحاق بها. كما أكدت الدراسات التي أصدرها الاتحاد الدولي في تموز ٢٠١٧ أن هناك ضرورة ملحة فى مجالات التعليم والتدريب والدراسات لرفع مستوى المهارات والمعرفة فى الأمن، إلى جانب إن هناك أربع فئات رئيسة للتهديدات السيبرانية للأمن القومى هى: الحرب السيبرانية والتجسس الاقتصادي (وهما مرتبطان بالحكومات)، وفئة الجريمة السيبرانية، والإرهاب السيبراني (اللذان يرتبطان في الأغلب بجهات دولية فاعلة غير تابعة لحكومة بذاتها).

ومن الأبعاد الاجتماعية الضرورية هي الحماية من تدنى المستويين القومي والأخلاقي في المجتمع. فالمحتويات غير المشروعة وغير المرغوب بها ذات تأثير سلبي على أخلاقيات المجتمع وعلى ارتفاع نسبة الممارسات الإجرامية كالإباحية، والترويج للإتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدولي. وعلبه، لا بد من بناء مجتمع مسؤول، ومدرك لمخاطر الفضاء السيبيرانى، قادرٌ مكن أن تترتب على التعامل مع قواعد السلامة ومدرك للعواقب القانونية، التي تعرض لسلامة الأفراد والمؤسسات ورؤوس الموال.

إن المخاطر الطويلة لأجل للمجتمع تمثل عنصرا جوهريا يجب دراسته. فقد تستمر الهجمات لبضع ثوان، ولكنها تحدث آثارا واسعة. وقد تتطلب الخسارة المجتمعية للثقة في هذه الثواني سنوات لاعادة بنائها. إن تقويض الثقة بين المواطنين والشركات وبين الدول نفسها يمكن ان يولد آثارا مدمرة على المجتمعات وعلى

الاستقرار العالمي في الاجل الطويل، عندها لا نستطيع ان نتحمل تكلفة الركود في هذا المجال بسبب ضياع الثقة. ويرجع ذلك لاســـباب من أهمها نقص الخبرة في التعامل في مثل هذه القضـــايا وقلة الوعي من قبل المســتهدفين، مما يزيد فرصـــة وجود جرائم الكترونية بشــكل كبير، ولمحاربتها يجب تطبيق ســياســة الامن السيبراني.

References:

[1] Imperva. (2021, November 9). What is Cyber Warfare | Types, Examples & Mitigation | Imperva. https://www.imperva.com/learn/application-security/cyber-warfare/

[2] TechTarget. (2023, March 9). What is Cyberwarfare? | Definition from TechTarget. https://www.techtarget.com/searchsecurity/definition/cyberwarfare

[3] Merriam-Webster. (2023, August 29). Cyber Warfare Definition & Meaning - Merriam-Webster. https://www.merriam-webster.com/dictionary/cyber%20warfare

[4] Khan, S. A. (2019). Cyber warfare as a non-kinetic threat: implications for Pakistan. ResearchGate. https://www.researchgate.net/publication/350387403_CYBER_WARFARE_AS_A_NON-KINETIC_THREAT_IMPLICATIONS_FOR_PAKISTAN

[5] ThreatCop. (2022). Cyber Warfare: Definition, Types, Examples, and Mitigation. Retrieved September 20, 2023, from https://threatcop.com/blog/cyber-warfare/

[6] The Heritage Foundation. (2022, October 18). Cyber Warfare and U.S. Cyber Command. The Heritage Foundation. https://www.heritage.org/military-strength/assessment-us-military-power/cyber-warfare-and-us-cyber-command

[7] The Conversation. (2017, October 18). The difference between cybersecurity and cybercrime, and why it matters. https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654

[8] MakeUseOf. (2021, January 16). What Is Cyberwarfare, Cyberterrorism, and Cyberespionage? MakeUseOf. https://www.makeuseof.com/what-are-cyberwarfare-cyberterrorism-and-cyberespionage/

[9] Eoyang, M., & Keitner, C. (2021, February 2). Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity. Journal of National Security Law & Policy. https://jnslp.com/2021/02/02/cybercrime-vs-cyberwar-paradigms-for-addressing-malicious-cyber-activity/

[10] Fortinet. (2012, June 1). What Is Cyberwarfare? Retrieved from https://www.fortinet.com/resources/cyberglossary/cyber-warfare

[11] Kaspersky. (2020, March 4). What is Cyber Security? | Definition, Types, and User Protection. Kaspersky. https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security

[12] IBM. (2022). Cybersecurity. Retrieved from https://www.ibm.com/topics/cybersecurity

[13] Cisco. (2017, August 18). What Is Cybersecurity? Cisco. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[14] KnowledgeHut. (2023, September 5). Importance of Cyber Security: Need and Benefits. KnowledgeHut. https://www.knowledgehut.com/blog/security/importance-of-cyber-security

[15] Sprinto. (2021, May 4). Importance of Cyber Security: Why is Cyber Security Important? Sprinto. https://sprinto.com/blog/importance-of-cyber-security/

[16] University of Tulsa. (2021, February 23). Why Is Cybersecurity Important? Top Six Reasons. University of Tulsa. https://cybersecurityonline.utulsa.edu/blog/why-is-cybersecurity-important-top-six-reasons/

[17] Digital Guardian. (2022). What is Cyber Security? Digital Guardian. https://www.digitalguardian.com/blog/what-cyber-security

[18] Cybersecurity and Infrastructure Security Agency (CISA). (2022, December 18). Cybersecurity Best Practices. https://www.cisa.gov/topics/cybersecurity-best-practices

[19] Information Security Office, University of California, Berkeley. (2022). Top 10 Secure Computing Tips. University of California, Berkeley. https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips

[20] National Institute of Standards and Technology. (2022). Cybersecurity measurement. Retrieved September 20, 2023, from https://www.nist.gov/cybersecurity-measurement

[21] Security Magazine. (2022, April 15). Cyber warfare: How to empower your defense strategy with threat intelligence. Security Magazine. https://www.securitymagazine.com/articles/97432-cyber-warfare-how-to-empower-your-defense-strategy-with-threat-intelligence

[22] Heimdal Security. (2023, June 22). The Cyber Kill Chain (CKC) Explained. Heimdal Security. https://heimdalsecurity.com/blog/cyber-kill-chain-model/

[23] EC-Council. (2022, January 1). The Cyber Kill Chain: The Seven Steps of a Cyberattack. EC-Council. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

[24] CrowdStrike. (2022, October 14). What is the Cyber Kill Chain? Introduction Guide. CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/

[25] SentinelOne. (2021, August 2). What is the Cyber Kill Chain? Steps, Examples, & How to Use It. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/

[26] BeyondTrust. (2018). What is the Cyber-Attack Chain, or Cyber Kill Chain? BeyondTrust. https://www.beyondtrust.com/resources/glossary/cyber-attack-chain

[27] Imperva. (2023, March 14). What is APT (Advanced Persistent Threat) | APT Security | Imperva. Imperva. https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

[28] Cisco. (2023, March 1). What Is an Advanced Persistent Threat (APT)? - Cisco. Cisco. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html

[29] KnowledgeHut. (2023, September 5). Advanced Persistent Threat: Examples, Detection, Prevention. KnowledgeHut. https://www.knowledgehut.com/blog/security/advanced-persistent-threat

[30] Cyberspaces Tech. (2022). Advanced Persistent Threats (APTs). Cyberspaces Tech. https://cyberspaces.tech/advanced-persistent-threats/

[31] BMC Blogs. (2022). Advanced Persistent Threats: Definition, Examples, and Prevention. BMC Blogs. https://www.bmc.com/blogs/advanced-persistent-threats/

[32] Clingendael. (2015). Foreign Policy Responses to Advanced Persistent Threats. Clingendael. https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf

[33] Brookings Institution. (2022, May 11). Legal Regimes Governing Cyberactivity and Cyberwarfare. Brookings Institution. https://www.brookings.edu/articles/legal-regimes-governing-cyberactivity-and-cyberwarfare/

[34] United Nations. (2023, June 1). Towards Cyberpeace: Managing Cyberwar Through International Cooperation. The UN Chronicle. https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

[35] InformationWeek. (2018, February 28). The Impact of Cyberwarfare. InformationWeek. https://www.informationweek.com/it-life/the-impact-of-cyberwarfare

[36] UNODC. (2018, January 25). Cybercrime Module 8 Key Issues: International Cooperation on Cybersecurity Matters. UNODC. https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

[37] Brookings Institution. (2022, May 11). Legal Regimes Governing Cyberactivity and Cyberwarfare. Brookings Institution. https://www.brookings.edu/articles/legal-regimes-governing-cyberactivity-and-cyberwarfare/

[38] RAND Corporation. (2022, April 29). Cyber Warfare. RAND Corporation. https://www.rand.org/topics/cyber-warfare.html

[39] Cybersecurityguide.org. (2023). Cyberwarfare. https://cybersecurityguide.org/resources/cyberwarfare/

[40] Carr, M. (2016). The Globalisation of Cybercrime: Understanding the Interconnectedness of an Increasing Threat. Chatham House. https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

[41] U.S. Government Publishing Office. (2014). Cybersecurity: Preparing for and Responding to the Enduring Threat. https://www.govinfo.gov/content/pkg/CHRG-113shrg88180/html/CHRG-113shrg88180.htm

[42] TeckPath. (2022, August 12). The Importance of Cyber Security for Non-Profit Organizations. TECKPATH | Managed IT Services | Business IT Support | Calgary IT Support. https://teckpath.com/the-importance-of-cyber-security-for-non-profit-organizations/

[43] Forbes Tech Council. (2022, November 8). The Necessity of Cybersecurity in The Nonprofit Sector. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/11/08/the-necessity-of-cybersecurity-in-the-non-profit-sector/

[44] CSO Online. (2022, October 18). Altruism under attack: why cybersecurity has become essential to humanitarian nonprofits. CSO Online. https://www.csoonline.com/article/573897/altruism-under-attack-why-cybersecurity-has-become-essential-to-humanitarian-nonprofits.html

[45] CSIS. (2022, March 22). A Shared Responsibility: Public-Private Cooperation for Cybersecurity. CSIS. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity

[46] World Economic Forum. (2022). The Business Imperative of Cyber Information Sharing. https://www3.weforum.org/docs/WEF_The_Business_Imperative_of_Cyber_Info_Sharing_2022.pdf

[47] Forbes Tech Council. (2022, November 8). The Necessity of Cybersecurity in The Nonprofit Sector. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/11/08/the-necessity-of-cybersecurity-in-the-non-profit-sector/?sh=2c13f1f95588

[48] eSecurity Planet. (2022, February 28). Cybersecurity Predictions for 2023. eSecurity Planet. https://www.esecurityplanet.com/trends/cybersecurity-predictions-2023/

[49] Ekran System. (2022, March 15). 12 Cybersecurity Best Practices to Prevent Cyber Attacks in 2023. Ekran System Blog. https://www.ekransystem.com/en/blog/best-cyber-security-practices

[50] Harvard Business Review. (2017, April 25). 8 Ways Governments Can Improve Their Cybersecurity. Harvard Business Review. https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity

[51] The White House. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[52] J.P. Morgan. (2022). The Threat of Business Email Compromise in the Public Sector. J.P. Morgan Insights. https://www.jpmorgan.com/insights/cybersecurity/business-email-compromise/threat-public-sector

[53] McKinsey & Company. (2020, September 16). Follow the Leaders: How Governments Can Combat Intensifying Cybersecurity Risks. McKinsey & Company Insights. https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

[54] Securities and Exchange Commission. (2015, October 19). The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses. SEC.gov. https://www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses

[55] IronNet Cybersecurity. (2022). Collective Defense for advanced cybersecurity. IronNet Cybersecurity. https://www.ironnet.com/topics/what-is-cyber-defense

Bibliography

Cyber Warfare:

1. Khan, S. A. (2019). Cyber warfare as a non-kinetic threat: implications for Pakistan. ResearchGate. https://www.researchgate.net/publication/350387403_CYBER_WARFARE_AS_A_NON-KINETIC_THREAT_IMPLICATIONS_FOR_PAKISTAN
2. ThreatCop. (2022). Cyber Warfare: Definition, Types, Examples, and Mitigation. https://threatcop.com/blog/cyber-warfare/
3. Imperva. (2021, November 9). What is Cyber Warfare | Types, Examples & Mitigation | Imperva. https://www.imperva.com/learn/application-security/cyber-warfare/
4. The Heritage Foundation. (2022, October 18). Cyber Warfare and U.S. Cyber Command. https://www.heritage.org/military-strength/assessment-us-military-power/cyber-warfare-and-us-cyber-command
5. TechTarget. (2023, March 9). What is Cyberwarfare? | Definition from TechTarget. https://www.techtarget.com/searchsecurity/definition/cyberwarfare
6. Merriam-Webster. (2023, August 29). Cyber Warfare Definition & Meaning - Merriam-Webster. https://www.merriam-webster.com/dictionary/cyber%20warfare

Cybersecurity:

7. BeyondTrust. (2018). What is the Cyber-Attack Chain, or Cyber Kill Chain? https://www.beyondtrust.com/resources/glossary/cyber-attack-chain
8. BMC Blogs. (2022). Advanced Persistent Threats: Definition, Examples, and Prevention. https://www.bmc.com/blogs/advanced-persistent-threats/

9. Brookings Institution. (2022, May 11). Legal Regimes Governing Cyberactivity and Cyberwarfare. https://www.brookings.edu/articles/legal-regimes-governing-cyberactivity-and-cyberwarfare/
10. Brookings Institution. (2022, May 11). Legal Regimes Governing Cyberactivity and Cyberwarfare. https://www.brookings.edu/articles/legal-regimes-governing-cyberactivity-and-cyberwarfare/
11. Carr, M. (2016). The Globalisation of Cybercrime: Understanding the Interconnectedness of an Increasing Threat. Chatham House. https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf
12. Cisco. (2017, August 18). What Is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
13. Cisco. (2023, March 1). What Is an Advanced Persistent Threat (APT)? - Cisco. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html
14. Clingendael. (2015). Foreign Policy Responses to Advanced Persistent Threats. https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf
15. CrowdStrike. (2022, October 14). What is the Cyber Kill Chain? Introduction Guide. https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/
16. Cybersecurity and Infrastructure Security Agency (CISA). (2022, December 18). Cybersecurity Best Practices. https://www.cisa.gov/topics/cybersecurity-best-practices
17. Cybersecurityguide.org. (2023). Cyberwarfare. https://cybersecurityguide.org/resources/cyberwarfare/
18. Cyberspaces Tech. (2022). Advanced Persistent Threats (APTs). https://cyberspaces.tech/advanced-persistent-threats/
19. Digital Guardian. (2022). What is Cyber Security? https://www.digitalguardian.com/blog/what-cyber-security
20. EC-Council. (2022, January 1). The Cyber Kill Chain: The Seven Steps of a Cyberattack. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/
21. Eoyang, M., & Keitner, C. (2021, February 2). Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity. Journal of National Security Law & Policy. https://jnslp.com/2021/02/02/cybercrime-vs-cyberwar-paradigms-for-addressing-malicious-cyber-activity/
22. Fortinet. (2012, June 1). What Is Cyberwarfare? https://www.fortinet.com/resources/cyberglossary/cyber-warfare
23. Heimdal Security. (2023, June 22). The Cyber Kill Chain (CKC) Explained. https://heimdalsecurity.com/blog/cyber-kill-chain-model/
24. IBM. (2022). Cybersecurity. https://www.ibm.com/topics/cybersecurity
25. Imperva. (2023, March 14). What is APT (Advanced Persistent Threat) | APT Security | Imperva. https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
26. Information Security Office, University of California, Berkeley. (2022). Top 10 Secure Computing Tips. https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
27. InformationWeek. (2018, February 28). The Impact of Cyberwarfare. https://www.informationweek.com/it-life/the-impact-of-cyberwarfare

28. Kaspersky. (2020, March 4). What is Cyber Security? | Definition, Types, and User Protection. https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security
29. KnowledgeHut. (2023, September 5). Advanced Persistent Threat: Examples, Detection, Prevention. https://www.knowledgehut.com/blog/security/advanced-persistent-threat
30. KnowledgeHut. (2023, September 5). Importance of Cyber Security: Need and Benefits. https://www.knowledgehut.com/blog/security/importance-of-cyber-security
31. MakeUseOf. (2021, January 16). What Is Cyberwarfare, Cyberterrorism, and Cyberespionage? https://www.makeuseof.com/what-are-cyberwarfare-cyberterrorism-and-cyberespionage/
32. National Institute of Standards and Technology. (2022). Cybersecurity measurement. https://www.nist.gov/cybersecurity-measurement
33. RAND Corporation. (2022, April 29). Cyber Warfare. https://www.rand.org/topics/cyber-warfare.html
34. Security Magazine. (2022, April 15). Cyber warfare: How to empower your defense strategy with threat intelligence. https://www.securitymagazine.com/articles/97432-cyber-warfare-how-to-empower-your-defense-strategy-with-threat-intelligence
35. SentinelOne. (2021, August 2). What is the Cyber Kill Chain? Steps, Examples, & How to Use It. https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/
36. Sprinto. (2021, May 4). Importance of Cyber Security: Why is Cyber Security Important? https://sprinto.com/blog/importance-of-cyber-security/
37. The Conversation. (2017, October 18). The difference between cybersecurity and cybercrime, and why it matters. https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654
38. U.S. Government Publishing Office. (2014). Cybersecurity: Preparing for and Responding to the Enduring Threat. https://www.govinfo.gov/content/pkg/CHRG-113shrg88180/html/CHRG-113shrg88180.htm
39. United Nations. (2023, June 1). Towards Cyberpeace: Managing Cyberwar Through International Cooperation. The UN Chronicle. https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation
40. University of Tulsa. (2021, February 23). Why Is Cybersecurity Important? Top Six Reasons. https://cybersecurityonline.utulsa.edu/blog/why-is-cybersecurity-important-top-six-reasons/
41. UNODC. (2018, January 25). Cybercrime Module 8 Key Issues: International Cooperation on Cybersecurity Matters. https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

Cybersecurity for Nonprofit Organizations:

42. CSIS. (2022, March 22). A Shared Responsibility: Public-Private Cooperation for Cybersecurity. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity
43. CSO Online. (2022, October 18). Altruism under attack: why cybersecurity has become essential to humanitarian nonprofits. https://www.csoonline.com/article/573897/altruism-under-attack-why-cybersecurity-has-become-essential-to-humanitarian-nonprofits.html
44. Ekran System. (2022, March 15). 12 Cybersecurity Best Practices to Prevent Cyber Attacks in 2023. https://www.ekransystem.com/en/blog/best-cyber-security-practices
45. eSecurity Planet. (2022, February 28). Cybersecurity Predictions for 2023. https://www.esecurityplanet.com/trends/cybersecurity-predictions-2023/

46. Forbes Tech Council. (2022, November 8). The Necessity of Cybersecurity in The Nonprofit Sector. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/11/08/the-necessity-of-cybersecurity-in-the-non-profit-sector/
47. Harvard Business Review. (2017, April 25). 8 Ways Governments Can Improve Their Cybersecurity. https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity
48. IronNet Cybersecurity. (2022). Collective Defense for advanced cybersecurity. https://www.ironnet.com/topics/what-is-cyber-defense
49. J.P. Morgan. (2022). The Threat of Business Email Compromise in the Public Sector. J.P. Morgan Insights. https://www.jpmorgan.com/insights/cybersecurity/business-email-compromise/threat-public-sector
50. McKinsey & Company. (2020, September 16). Follow the Leaders: How Governments Can Combat Intensifying Cybersecurity Risks. McKinsey & Company Insights. https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks
51. Securities and Exchange Commission. (2015, October 19). The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses. SEC.gov. https://www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses
52. TeckPath. (2022, August 12). The Importance of Cyber Security for Non-Profit Organizations. TECKPATH | Managed IT Services | Business IT Support | Calgary IT Support. https://teckpath.com/the-importance-of-cyber-security-for-non-profit-organizations/
53. The White House. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
54. World Economic Forum. (2022). The Business Imperative of Cyber Information Sharing. https://www3.weforum.org/docs/WEF_The_Business_Imperative_of_Cyber_Info_Sharing_2022.pdf