السياسات العامة للأمن السيبراني في مملكة بلجيكا: الواقع والمستقبل

م.د سامر ناهض خضير
جامعة النهرين / كلية العلوم السياسية
samer.nahed@nahrainuniv.edu.iq

الملخص:

لقد واجهة الحكومة البلجيكية تحديات الأمن السيبراني، جراء الثورة التقنية التي حولت انشطتها من الاجراءات التقليدية الى اجراءات رقمية يتم التعامل معها من خلال اجهزة وبرامج، تنتقل عبر شبكات الكترونية وتحفظ في ذاكرة بيانية، ما اعادة ذلك رسم مفهوم الأمن من جديد. هذا المفهوم الجديد تتطلب من الحكومة البلجيكية صنع سياسات تتعاطى مع هذا المتغير الذي طرئ على نشاطات الدولة بالشكل الذي يوفر لها الحماية الكافية من التهديدات السيبرانية، وما كان للحكومة البلجيكية الا ان تصدر جملة من السياسات التي أُنتج عنها تأسيس المركز الوطني للأمن السيبراني، الذي ينصب عمله على توفير مستلزمات الحماية من اجهزة وانظمة وبرامج الكترونية وتوعية للمواطنين، فضلاً عن دوره في تعزيز سبل التنسيق والتعاون بين المؤسسات المحلية والدولية من اجل مواجهة الهجمات السيبرانية، مع ذلك فان كل هذه الاجراءات التي تقوم بها الحكومة البلجيكية تكون وليدة من السياسات التي يعتمدها الاتحاد الأوروبي. لذا جاء هذا البحث ليتناول سياسة الأمن السيبراني في بلجيكا منذ بداية تأسيسها؛ وصول الى مراحل تطورها وتنوعها، والى اليات انفاذها، وكذلك المستقبل المتوقع لها.

الكلمات المفتاحية: السياسات العامة، الأمن السيبراني، الحكومة، العالم الافتراضي، التقنية.

Cybersecurity Public Policy in the Kingdom of Belgium: Reality and Future

Lecturer Dr. Samer Nahedh Khudhair
University of Nahrain / College of Political Science
samer.nahed@nahrainuniv.edu.iq

Abstract:

The Belgian government has faced cybersecurity challenges due to the technological revolution that transformed its activities from traditional procedures to digital procedures that are dealt with through devices and programs that are transmitted over electronic networks and stored in a graphic memory, which redraws the concept of security anew. This new concept requires the Belgian government to create policies that deal with this variable that has occurred in the state's activities in a way that provides it with adequate protection from cyber threats. The Belgian government had no choice but to

issue a set of policies that resulted in the establishment of the National Cybersecurity Center, whose work focuses on providing protection requirements from electronic devices, systems, and programs and raising awareness for citizens, in addition to its role in enhancing means of coordination and cooperation between local and international institutions in order to confront cyber-attacks. However, all these measures taken by the Belgian government are the result of the policies adopted by the European Union. Therefore, this research came to address the cybersecurity policy in Belgium since its inception; reaching the stages of its development and diversity, and its enforcement mechanisms, as well as its expected future. **Keywords:** (Public policy, cybersecurity, government, virtual world, technology).

المقدمة:

لقد اعادة التقنية صنع السياسات العامة للأمن بصيغ وممارسات لا تنتمي الى أسلوب تحقيقها من قبل، لأنها اوجدت نمط حياة مغاير في تحدياته؛ التي لا تنصاع الى ابعاد مكانية وزمانية؛ انما الى بيئات رقمية تعمل بواسطة اجهزة الكترونية، تتعامل مع معلومات بيانية تحفظ في حاويات بيانية وتنتقل عبر شبكات الكترونية، يمكن اختراقها بأنظمة وبرامج يصعب احتوائها او مواجهتها.

إن هذا التحدي الذي ولده العالم الافتراضي يزداد بشكل كبير مع دولة بلجيكا، باعتبارها موطناً لمؤسسات الاتحاد الاوربي وحلف الشمال الاطلسي والمقر الاعلى للقوى المتحالفة في اوروبا، مما شكلت هدفاً جذاباً للتجسس الالكتروني او التخريب في المجالات السياسية والاقتصادية والاجتماعية، جعل منها ان تكون في مواجهة مستمرة لهذا التحدي، ما الزمها على وضع التدابير اللازمة المتمثلة في صنع السياسات العامة من اجل تأسس منظومة امن سيبراني؛ تأخذ بنظر الاعتبار حجم التهديد الذي يواجه الافراد والمؤسسات والمنظومة التحتية لها المتمثلة بالمستشفيات ومحطات الكهرباء والمياه والمصارف وغيرها. ومع ذلك فإن اداء وكفاءة صنع السياسات العامة يعتمد في الاساس على مدى تفاعل مؤسسات النظام السياسي البلجيكي في مواجهة واحتواء التهديدات السيبرانية.

لذا يسعى هذا البحث الى الغوص في اعماق السياسات العامة المتبعة في بلجيكا، لمعرفته اساليبها، وسبل مواجهتها لتحديات الأمن السيبراني الذي تواجهه الدولة.

أهمية البحث.

تكمن اهمية البحث على النحو الاتي:

١- تقديم رؤية عن الاطار العام للسياسات العامة التي تعتمدها الحكومة البلجيكية في مجال الأمن السيبراني.

٢- يركز البحث على معرفة طبيعة التعاون والتنسيق التي اتبعتها السياسات العامة للأمن السيبراني في مملكة بلجيكا.

٣- تسليط الضوء، على الطريقة التي تعتمدها الحكومة البلجيكية، في مواجهة التهديدات السيبرانية.

اهداف البحث.

ان ابرز الاهداف التي يسعى اليها البحث هي:

١- دراسة تجربة مهمة في مجال صنع السياسات العامة للأمن السيبراني في مملكة بلجيكا، يمكن ان يستفد منها صانع القرار العراقي في صنع سياسة فعالة لمواجهة التهديدات السيبرانية.

٢- فتح المجال امام الباحثين للانطلاق نحو توسيع الدراسات في مجال التقنية الالكترونية من خلال ربط هذه المتغيرات بعمل الدولة والحكومة.

اشكالية البحث.

على الرغم من الجهود التي تقوم بها الحكومة البلجيكية في صنع السياسات العامة من اجل حماية امنها السيبراني، الا انها لا تزال هناك اشكاليات تتعلق بمدى جاهزية البنية التحتية السيبرانية، وفعالية التدابير الوقائية والدفاعية التي تستخدمها في مواجهة التهديدات السيبرانية. لذا نكون امام سؤال جوهري هو كيف يمكن للحكومة البلجيكية صناعة سياسات عامة استراتيجية، تقوم على الصمود ام الهجمات السيبرانية؟.

فرضية البحث.

إن السياسات العامة للأمن السيبراني في مملكة بلجيكا، يمكن ان تصبح فعالة، اذا تعاطت مع تحديات الأمن السيبراني عن طريق اتباع نهج كامل؛ يعمل على انشاء بنية تحتية متكاملة، واجراء تحديث مستمر للسياسات، فضلاً عن تعزيز التنسيق والتعاون بين القطاع الخاص والعام من جهة، والحكومة البلجيكية مع مؤسسات الاتحاد الاوروبي لمواجهة التهديدات السيبرانية من جهة اخرى.

منهجية البحث.

اعتمد البحث على منهج التحليل النظمي.

هيكلية البحث.

قسم البحث على النحو الاتي:

اولاً: مفهوم السياسات العامة للأمن السيبراني.

ثانياً: رؤية عن صنع السياسات العامة للامن السيبراني في مملكة بلجيكا.

ثالثاً: مرتكزات السياسات العامة للأمن السيبراني في مملكة بلجيكا.

رابعاً: اهداف السياسات العامة للأمن السيبراني في مملكة بلجيكا.

خامساً: اليات انفاذ السياسيات العامة في مملكة بلجيكا.

سادساً: مستقبل السياسات العامة للأمن السيبراني في مملكة بلجيكا.

اولاً: مفهوم السياسات العامة للأمن السيبراني.

مع ولادة الالفية الثالثة اتجهت اهتمامات الدول نحو صنع سياسات امن جديدة تتعلق باساليب امنية مستحدثة ذات ابعاد بيانية تعمل في عالم افتراضي عرف باسم (الفضاء السيبراني) الذي يعبر عن نظام اجتماعي تقني معقد يوازي العالم الواقعي في استخداماته(Karyda 2017, 3) .

تجسدت تلك السياسة في مفاهيم متعددة عبرت عن وجهات نظر مختلفة جراء حداثة النشأة لمفهوم الأمن السيبراني والصعوبة في تحديد مدلولاته ونطاق عمله. فلم يعد مفهوم الأمن يرتبط بتوفير الحماية اللازمة للموجودات، انما مفهوم الأمن في عالم التقنية الالكترونية اخذ منحى اخر يتعلق بالبيانات والانظمة والبرامج التي اضحت تعبير عن اعمال الدولة وخصوصيات افراد المجتمع، لذا اصبح يعبر عنه بـ" تأمين البرامج والشبكات والانظمة من الهجمات السيبرانية" ما يشير ذلك الى الانتقالة التي احدثتها التقنية في مزاولة الاعمال من العالم الواقعي الى الشبكات الالكترونية التي اختلفت معها نوعية وطبيعة المخاطر والتهديدات التي تتعرض لها البيانات الالكترونية التي تتبادل او تحفظ في اجهزة الكمبيوتر وما شابهها من اجهزة اخرى التي يمكن اختراقها وسرقتها عن طريق الهجمات السيبرانية، ما ضاعف الجهد على الدول في اعداد السياسات لصد ومواجهة الهجمات والاختراقات في عالم لا تحدد ابعاده واساليبه. (Eriksson and Giampiero 2022, 98).

وبذلك تكون السياسات العامة للأمن السيبراني ممارسة لتحديد نقاط الضعف المحتملة سواء اكانت في التقنية او المستخدم، ووضع المعالجة المناسبة لها للحد من تأثير التهديدات المحتملة (Cavelty and Wenger 2022 ,7-9). او انها عملية توفير التقنيات والاشخاص المختصين لحماية البنية التحتية للأنظمة الالكترونية (Wenger and Cavelty 2022, 247-251). ويتبين ان هذا النوع من السياسات العامة يرتكز على عنصرين اساسين الاول توفير التقنية من اجهزة الكترونية، وبرامج تتطلب مواكبة التغيرات والتطورات الحاصلة والمستخدمة في الهجمات الالكترونية، والثاني العنصر الانساني الواعي لحجم المخاطر في العالم الافتراضي.

وفي هذا الصدد اخذت السياسات العامة التي تقوم الحكومة على اعدادها في وضع اطر عامة وخاصة في التعامل مع التهديدات السيبرانية، فضلاً عن اعداد المستخدم المتمثل بالفرد والمؤسسات على توجيه اهتماماتهم بالمخاطر التي يتطلب مواجهتها والحد منها(Baezner and Cordey 2022: Cavelty and Wenger 22-25)

لذا فان طبيعة صنع السياسات العامة وطريقة عملها بشكل فعال سوف تتعلق بطبيعة الدولة ونوعية نظامها السياسي وتركيبتها الاجتماعية وطبيعة استخدامها للتقنية وحجم علاقاتها وتفاعلاتها مع العالم وطبيعة الوعي لدى افراد المجتمع (Steed 2022, 206)، فمن أجل تأمين الفضاء الإلكتروني يتطلب وجود تثقيف لكل مستخدم للانترنت حول المخاطر السيبرانية، من هنا ظهر مفهوم "النظافة السيبرانية" كخط الدفاع الأول ولأكثر فعالية وبناء مشترك ومتين في سياق أمن المعلومات الأوسع، بهدف توحيد الفهم والأساليب لدعم وتقليل المخاطر المتعلقة بالأمن السيبراني داخل المجتمع، الذي ينبغي أن يقوم على بناء أساس متين لثقافة النظافة السيبرانية السليمة والأمنة في المستقبل(Gruschka 2018,302). فضلاً عن وجود اتجاه اخر في تعريف السياسة العامة للأمن الالكتروني الذي يرى "انها عملية جماعية تنمو وتتغير مع مرور الوقت حسب متطلبات البيئة وطبيعة التهديد " (Steiger 2022,143-146) . ذهب هذا التعريف الى جعل هذه السياسية عملية ديناميكية تتغير مع ظروف الزمان والمكان في مواجه المخاطر.

وبناء على ذلك فان صنع سياسات عامة فعالة ينبع من ادراك الدولة لحجم المخاطر التي تسببها التهديدات السيبرانية، ما يدفعها الى وضع الاليات المناسبة للحد منها(Karyda 2017, 3). والانتقال من الاجراءات البسيطة الى اجراءات رصينة تكون موضع ثقة في حماية البيانات، ما يجعل منها ان تكون نظام يتم فيه التوجيه والتحفيز والمعرفة الفعلية بأمن المعلومات .Kuerbis and other) 2022,231).

وبذلك تكون معايير السياسات العامة الفعالة تتمثل في وجود اطر مؤسساتية مدروسة تقوم بين الحين والاخر على اجراء التقييم لادواتها وطرق عملها واجراء التقويم بناء على النتائج المترتبة على ذلك (Bonfanti 2022, 66))، والذي يتمثل ذلك في اجراء استبيان او طرح فايروس الكتروني وملاحظة طرق التعامل معه او طرح اشاعة حول موضوع ما وانتظار ردود الافعال حوله. فضلاً عن اعتمادها على الاطر العامة، المتمثلة بالمعايير الدولية والخاصة التي تتمثل بعادات وتقاليد وقيم المجتمع (Cavelty and Wenger 2022,4).

ومع ذلك فان هذا النوع من السياسات العامة ليست كالسياسات الاخرى التي تعيش داخل البيئة القانونية. فان السياسة العامة للأمن السيبراني تتطلب الى معرفة ووعي ليتم التعايش معها، لان العالم الافتراضي، لا يمكن حصره وفقاً لمحددات زمانية او مكانية، مما يتطلب تعامل من نوع خاص Karyda) (2017, 4).

في النهاية ترتكز السياسة العامة لامن التقنيات الرقمية على ممارسات ادارة المخاطر التي طورها مختصون في مجال الكمبيوتر، لجعل اجهزة الكمبيوتر والشبكات الالكترونية اكثر اماناُ، ما يدل على ان

الأمن السيبراني يكون اكثر من كونه مجرد امن معلومات، فانه يمتد الى امن البشر بمختلف تفاصيلها المالية والعملية والعلمية، لذا فالأمن في هذه التفصيلة، ينطلق من اعتبارين تقني وانساني في سبيل اعداد معادلة مترابطة ومتفاعلة، تنتج تأثير متبادل يوازي بين العنصرين.

يمكن التوصل الى ان مفهوم سياسات الأمن الالكتروني: مجموعة من الاجراءات والاهداف والمبادئ التي تقوم الدولة على صنعها من اجل مواجهة التهديدات السيبرانية.

ثانياً: رؤية عن صنع السياسات العامة للامن السيبراني في مملكة بلجيكا.

لقد استوعبت الحكومة البلجيكية حجم المخاطر التي رافقت انتقال عمل الدولة، من الاجراءات التقليدية التي تتطلب جهد ووقت وتكاليف عالية، الى اعمال تسير بصيغة بيانات الكترونية يتم التعامل معها من خلال اجهزة الكترونية تعمل على حفظ وتداول المعلومات، بهذه الطريقة من العمل برز تحدٍ من نوع جديد في عمل الدولة، تمثل ذلك في اختراق البيانات الالكترونية للافراد والمؤسسات ما اضحى ذلك يهدد امن الدولة بالكامل، وبطبيعة انتماء دولة بلجيكا الى الاتحاد الاوربي وما تجسد ذلك من دخول هذه البيئة على التعاطي والتعامل بشكل واسع وكبير مع متغير تكنلوجيا الاتصال والبرامج الالكترونية. دفعها في عام ١٩٩٨ جراء التهديدات المستمرة والمتزايدة الى انشاء (اللجنة البلجيكية لحماية الخصوصية) او (هيئة الخصوصية البلجيكية) (Commission for the Protection of Privacy) التابعة الى الحكومة والمسؤولة امام البرلمان، تقوم بمهام حماية بيانات الافراد الشخصية (Nunes 2023,124) .اعتمدت هذه الهيئة في تأسيسها على قانون حماية البيانات الشخصية في بلجيكا لعام ١٩٩٢ واللوائح الصادرة من الاتحاد الاوربي التي تتعلق بالبيانات الشخصية للافراد (Flkner And others 2021,154) وفي فبراير/شباط عام ٢٠٠٠ تم إنشاء مجموعة عمل مهمتها تقوم على دراسة امكانية انشاء وكالة فيدرالية في مجال التشفير وحماية المعلومات(Easttom 2021, 329) ، وسرعان ما خلصت إلى أنه لا يمكن انشاء مثل هذه الوكالة، بسبب القيود المالية (Newton 2010,1244) وفي عام ٢٠٠٥ تم ايجاد حل اخر يقوم على تطوير منصة تسمى (الشبكة البلجيكية لأمن المعلومات) (BelNIS) وهي منصة غير رسمية تتألف من ممثلي المؤسسات الحكومية وغير الحكومية، كان هدفها جمع المعلومات وتقديم التوصيات المتعلقة بأمن المعلومات وكذلك التثقيف حول مخاطر الأمن السيبراني وتعزيز التعاون بين القطاع العام والخاص في صد الهجمات الالكترونية (Jakobs 2009, 215) ولكن لم تُكلف بدور امان الشبكة الالكترونية انما خول الى (هيئة خدمة تكنلوجيا المعلومات والاتصالات) (FEDICT) وهي مؤسسة فدرالية حكومية في بلجيكا تقدم خدمة عامة لتكنولوجيا المعلومات والاتصالات تأسست في عام 2001 (Svard & Joshi 2015, 283-284).

وبالعودة الى منصة (الشبكة البلجيكية لامن المعلومات) نجد انها تبنت مفهوم المصفوفة الكاملة أو المشاركة بالكامل حيث وفرت الفرصة للخبراء الميدانيين من مختلف الوكالات الحكومية للقاء مرة واحدة في الشهر للمناقشة والتشاور مع بعضهم البعض حول القضايا المتعلقة بالأمن السيبراني (Rondelez, 2018, 307) .

يمكن القول إن المنصة عملت كمركز تواصل بين الاطراف المعنية في البلاد، لتحقيق هدف جماعي يكون من خلال تعزيز التعاون وتبادل المعلومات بين المؤسسات الحكومية وغير الحكومية في مجال تعزيز الأمن السيبراني في بلجيكا (Brown & Garson 2013, 213).

لم تكتفي الحكومة البلجيكية بهذا القدر من السياسات العامة في مواجهة التهديدات السيبرانية، فقد أنشأت في عام ٢٠١١ (فريق الاستجابة لحالات الطوارئ الحاسوبية) وعبرت في بيان انه المسؤول عن تطوير سياسة أمنية اتحادية تتعلق بشبكات وأنظمة المعلومات، من خلال مراقبتها وتحليل نوعية التهديد وتقديم الدعم الفني للجهات المستهدفة، واستمرت عملية تطوير امكانيات مواجهة التهديدات السيبرانية، ففي النصف الثاني من عام ٢٠١٢، قررت الحكومة إنشاء مجموعة عمل للتفكير في مقترحات لتطوير استراتيجية وطنية للأمن السيبراني، وفي ٣ أكتوبر ٢٠١٢ (Felkner and others 2021,154) ، قدمت السياسة الأولى للأمن السيبراني، وكلف مجلس الوزراء رئيس الوزراء – في ٢١ ديسمبر ٢٠١٢ – بتنسيق تنفيذ هذه السياسة (Rondelez, 2018, 307) ، التي تهدف الى تحقيق ثلاثة أهداف (Francisco and others 2021, 145):

١- وجود فضاء ألكتروني آمن وموثوق به .

٢- تحقيق أمن وحماية للبنى التحتية الحيوية، من خلال التعرف أولاً على التهديدات السيبرانية، وثانياً تعزيز سبل مكافحتها.

٣- تطوير قدرات الأمن السيبراني الوطني، من خلال وضع الاجراءات اللازمة للاستجابة للخروقات التي يتعرض لها الفضاء السيبراني.

وفي ٦ نوفمبر ٢٠١٣ – أعلنت الحكومة قرارها بتسريع تنفيذ سياسة الأمن السيبراني وإطلاق المبالغ المالية لإنشاء (المركز الوطني للامن السيبراني) (Centr for Cybersecurity (CCB) . وفي عام ٢٠١٤- اتخذت الحكومة قرارًا بشأن تخصيص الموارد له وبموجب ذلك بدأت أنشطته التشغيلية في يناير ٢٠١٥(Rondelez, 2018, 307).

جاء انشاء هذا المركز نتيجة زيادة حجم التهديدات السيبرانية كان ابرزها في يونيو ٢٠١٣ عندما تم الكشف عن اختراق شركة الاتصالات الوطنية البلجيكية التي كانت تسمى سابقًا (Belgacom) والتي تُعرف حاليًا باسم (Proximus) من قبل أجهزة استخبارات حليفة أو أجنبية مثل وكالة الأمن القومي الأمريكية (NSA) ومقر الاتصالات الحكومية البريطانية (GCHQ). الذي ابلغ الحكومة البلجيكية

باختراق وزارة الخارجية، قبل أسابيع قليلة من الانتخابات الوطنية لعام ٢٠١٤ . فضلاً عن الحاجة المتزايدة التي تفرضها البيئة الالكترونية (Guitton and others 2015,39).

يمكن القول: إن إنشاء (المركز الوطني للأمن السيبراني) في بلجيكا يشير إلى تغيير هائل في الطريقة التي يتم بها إدارة الأمن السيبراني. لأنه مَثل بداية نهج الحكومة بأكملها، الذي تجسد في توفير تنسيق متكامل ومركزي للأمن السيبراني، وبذلك فهي سياسية للحفاظ على مؤسسات القطاع العام والخاص من الاختراقات وإلى المزيد من التكامل والتنسيق. ويبدو من ذلك أن الحكومة البلجيكية إرادة أن تصبح منسقًا ومسيراً للأمن السيبراني.

ان التحليل يظهر من ذلك أن شبكة الأمن السيبراني البلجيكية تطورت من شبكة غير رسمية تحكم نفسها إلى شبكة هرمية رسمية تحكمها مؤسسات النظام السياسي بأنظمة الكترونية.

وفي ٣٠ يوليو ٢٠١٨ أقر البرلمان البلجيكي قانون حماية بيانات الأفراد الشخصية وحدد السلطة المسؤولة عن إنفاذه هو (المركز الوطني للامن السيبراني في بلجيكا)، هذا القانون حدد التكوين والمهام والصلاحيات للمركز الوطني، واعطى الصلاحية للمركز للنظر في الشكاوى وتقديم الارشادات وفرض الغرامات على المخالفين ويكون ذلك بالتعاون مع اللائحة العامة التي تقوم على حماية البيانات (GDPR) المطبقة على مستوى الاتحاد الاوربي. وتم تحديث هذا القانون مؤخرًا في (٢٠٢٣ –٢٠٢٤) من قبل البرلمان ايضاً لإصلاح التكوين الداخلي للهيئة التنظيمية (Couriel 2025 , 98) ، وعليه يقوم المركز الوطني بانفاذ هذا القانون بالتعاونً مع السلطات الإدارية، والقضائية، وأجهزة الاستخبارات، وخدمات الشرطة، وهذا القانون يشكل جزء من التزام بلجيكا مع سياسة الاتحاد الاوربي ويهدف الى تعزيز الأمن السيبراني من خلال التعاون بين مختلف الجهات(O'Neill & Swinton 2013, 28). وفي ٢٢مايو (٢٠٢١– ٢٠٢٥) قام مجلس الأمن القومي البلجيكي بأصدار سياسة محدثة بالتعاون مع (المركز الوطني للامن السيبراني) التي سعت الى جعل بلجيكا من اكثر الدول اماناً في اوروبا، لذا عملت على تعزيز حجم الاستثمارات في مجال التقنية الرقمية وتحسين الشراكة بين القطاع الخاص والعام والتشديد على الالتزام الدولي، ولضمان ذلك اوكلت مهام التنفيذ والرقابة والتنسيق والاشراف للمركز الوطني، لكنها في الوقت ذاته اشركت معه الجهات الفاعلة في مجال الأمن السيبراني وهم وحدة جرائم الكمبيوتر الاقليمية والمدعي العام وامن الدولة والشرطة الفيدرالية والمركز الوطني للازمات ومع ذلك يتم مراجعتها وتعديلها بشكل دوري وعند الضرورة (Mayer 2023,362).

واستمرت عملية تشريع القوانين في هذا الصدد اذ صدر (قانون التصديق على الأمن السيبراني) في ٢٠ يوليو ٢٠٢٢ من قبل البرلمان بشأن منح شهادة الأمن السيبراني لتقنيات المعلومات والاتصالات وكلف المركز الوطني بمنح هذه الشهادة، وكان الهدف منه تعزيز حماية الشركات من الهجمات

الالكترونية من خلال الايفاء بالمعايير التي وضعها القانون Cybersecurity Strategy Belgium) 2.0 2021,3).

يمكن القول: ان السياسة العامة للحكومة البلجيكية المتبعة في مجال الأمن السيبراني شهدت مراحل تطور عدة وهذا يعود الى طبيعة توسع عمل الدولة في مجال الفضاء السيبراني، فضلاً عن تحديث برامج وانظمة هجماته على مختلف قطاعات الدولة، ما تطلب ذلك الى اخذ التدابير اللازمة في مواجهة هذه التحديات، التي تمثلت في القوانين الصادرة من قبل البرلمان او السياسيات التي تقوم الحكومة على اصدارها من اجل الحد من الهجمات السيبرانية.

ثالثاً: مرتكزات السياسات العامة للأمن السيبراني في مملكة بلجيكا.

ان صنع كل هذه السياسات، تنطلق من وثيقة الدستور الذي يقوم عليه التنظيم السياسي والقانوني في بلجيكا، فقد نصت أحكامه بشكل واضح على حماية الحقوق والحريات الأساسية للمواطنين، وكذلك وامن الدولة بالكامل (المادة ٢٢)، مع ذلك فان هذه السياسية العامة لا تعتمد على حرية تامة في التعامل مع هذا التحدي السيبراني، لان بلجيكا بحكم عضويتها في الاتحاد الاوربي يفرض عليها ان تلتزم بالسياسة العامة التي يتم صنعها في الاتحاد، فهذه السياسية بعضها يتم تنفيذها على مستوى الدول، والتي تعكس حالة من التعاون والتناغم بين دول الاتحاد الأوروبي في اتخاذ تدابير وقاية ومواجهة، وكذلك عقوبات تفرض على مرتكبي الجرائم الالكترونية (Summers 2014 ,224) ، كان من اهم تلك السياسات العامة هو التوجيه المتعلق بالخصوصية الإلكترونية (eprivacy Directive) الذي هو عبارة عن تشريع صادر من قبل الاتحاد الاوربي، يهدف الى حماية الخصوصية في المجال الالكتروني، مثل الانترنت والبريد الالكتروني والاتصالات، فضلاً عن تنسيق أحكام الدول الأعضاء في الاتحاد الأوروبي لضمان مستوى كافي لحماية الخصوصية (Armstrong 2012,93).

وكذلك اللائحة العامة لحماية البيانات ٦٧٩/٢٠١٦ (GDPR) والصادرة عن البرلمان الأوروبي بتاريخ ٢٧ ابريل التي تعد بمثابة التشريع الشامل للاتحاد الأوروبي المصمم لحماية حقوق وخصوصية الأفراد المتعلقة في بياناتهم الشخصية، وتكون السلطة المسؤولة عن إنفاذها هي (هيئة حماية البيانات البلجيكية Autorité de protection des) (Langella and others 2023, 16) ، وايضاً توجيه ٢٠١٦/ ٦٨٠ الصادر عن الاتحاد الاوربي والذي يقوم على توجيه عمل الشرطة على مستوى دول الاتحاد في مجال التعاون من اجل منع الجرائم الالكترونية من خلال اكتشافها قبل حدوثها أو التحقيق فيها وفي حالة اثباتها تفرض العقوبات الجنائية على المخالفين(Chané and others 2020, 325)، وصدر كذلك توجيه أمن الشبكات والمعلومات ١١٤٨/٢٠١٦ ("NIS-١"). يعمل هذا التوجيه على تعزيز الأمن السيبراني ومواجهة تهديداته التي تستهدف المجال الصحي والطاقة والجانب المالي، وكذلك

المواصلات في جميع أنحاء الاتحاد الأوروبي، من خلال فرض قواعد أمن المعلومات لأنظمة الشبكات ولمشغلي الخدمات الأساسية. ولائحة EU/٢٠٢٠/١٥٠٣ التي تهدف الى تعزيز قدرات الأمن السيبراني والتعاون بين الاعضاء من الدول كل هذه التوجيهات غير قابلة للتطبيق بشكل مباشر من قبل الاتحاد الاوربي، لذا يجب نقلها إلى قانون الدولة العضو لانفاذها Belgium Cybersecurity Strategy (2.0 2021,31).

في حين البعض الاخر يكون تنفيذها من قبل مؤسسات الاتحاد حصراً مثل قانون الأمن السيبراني ٨٨١/٢٠١٩ (CSA). شرع هذا القانون من قبل الاتحاد الاوربي من اجل تعزيز قدرة الاتحاد على مواجهة التهديدات السيبرانية، كما ساهم في انشاء إطاراً أوروبياً مشتركاً يقوم على اصدار شهادات الأمن السيبراني لمنتجات وخدمات وعمليات تكنولوجيا المعلومات والاتصالات، وساهم ايضاً في تعزيز دور وكالة الأمن السيبراني التابعة للاتحاد الأوروبي (ENISA) (Goetry and others 2024)، التي تعد الهيئة الرئيسة في الاتحاد، والمسؤولة عن مواجهة الهجمات السيبرانية، والقيام بالتنسيق بين دول الاتحاد وبناء القدرات السيبرانية وتوجيه السياسات والتعاون بين القطاع العام والخاص ومنح شهادات الأمن السيبراني وتعمل على تطوير ثقافة وعي عام بامن الشبكات والمعلومات في الاتحاد (Akinwale & Afolayan 2017 ,56).

وبذلك فان صنع سياسة عامة للأمن السيبراني في بلجيكا اعتمدت اولاً على الدستور الذي اتاح حماية امن الدولة بشكل عام والفرد بشكل خاص، فضلاً عن مظلة الاتحاد الاوربي التي اسست منظومة واسعة من السياسات العامة في مجال بناء امن سيبراني انعكس ذلك على سياسة الحكومة البلجيكية في حماية امنها السيبراني. وبناءً على ذلك دعمت بلجيكا الدور التشريعي والدبلوماسي للاتحاد الاوربي والمؤسسات الدولية الاخرى ذات الصلة في مساهمتها لتأسيس بيئة سيبرانية مفتوحة حرة وامنة وتشارك بنشاط كلما امكن ذلك (Felkner and others 2021,154) .

بعد ان تناول البحث السياسة العامة للحكومة البلجيكية في التعامل مع التهديدات، فضلاً عن مرتكزاتها التي استندت عليها في الشروع الى صنعها، سيتناول البحث بعد ذلك اهم العناصر والاهداف التي استندت عليها.

رابعاً: اهداف السياسات العامة للأمن السيبراني في مملكة بلجيكا.

تقوم السياسات العامة للأمن السيبراني في بلجيكا على تحقيق مجموعة من الاهداف. يمكن تناولها على النحو الاتي:

١- بناء القدرات السيبرانية: تشير الى تطوير الامكانيات التقنية والبشرية والمؤسسية من اجل حماية الانظمة الرقمية من التهديدات السيبرانية، هذه الحماية تمثلت في انظمة كشف التهديدات وجدران

الحماية والتشفير المعقد هذا من جانب ومن جانب اخر وضع منظومة متكاملة من التشريعات التي تقوم على تأسس اليات انفاذ تعمل وفقاً للاطار المؤسساتي، فضلاً عن ذلك تحفيز عمليات البحث والابتكار في الجامعات ومراكز البحوث سواء اكان ذلك من خلال الدعم المالي الذي تقدمه الحكومة او عن طريق حث الشركات الربحية على الاستثمار في التقنية الالكترونية من اجل تقديم الحلول والتوصيات للتهديدات التي تتعرض لها(Fang 2018, 19).

٢- تعزيز الثقة: لقد وضعت الحكومة مسألة الثقة كواحدة من ابرز اهداف سياستها العامة. لذا ركزت على ايجاد بيئة سيبرانية امنة تشعر الافراد والمؤسسات ان بياناتهم الالكترونية محمية من الهجمات ولم يتم استغلالها لصالح الحكومة، ويكون ذلك عن طريق اعتمادها على الشفافية في اجراءات عملها التي تنطوي على نشر التقارير الدورية حول الهجمات الالكترونية والطريقة التي تتم مواجهتها (Santos. 2024, 478) .

٣- تعزيز التعاون مع الدول والمؤسسات الدولية: اعطت الحكومة البلجيكية اهمية بالغة في تعزيز فرص الاتصال والتواصل مع المجتمع الدولي، ولا سيما مع الاتحاد الاوربي من اجل ايجاد تشريعات موحدة تعمل على الحد من التحديدات السيبرانية، فضلاً عن تعزيز التعاون القانوني بين الدول من اجل تسهيل التحقيقات في الجرائم المرتكبة وتسليم المجرمين. ولا يقتصر الامر على ذلك انما يمتد الى تعزيز عملية تبادل المعلومات حول التهديدات السيبرانية من خلال عقد المؤتمرات الدورية او تأسيس منصات دولية من اجل مشاركة المعلومات (Group of authors 2021, 193)، او عن طريق التعاون الاستخباراتي الذي يعمل على الحد من عمليات التجسس او التلاعب في نتائج الانتخابات(Tan 2019, 129)، هذا التعاون لم يقتصر على الدول او المؤسسات الدولية انما حتى مع الشركات العالمية مثل مايكروسوفت وجوجل وغيرها من اجل مواجهة التهديدات السيبرانية (Paulus 2024, 89).

ان الاهداف التي سعت اليها السياسات العامة جاءت باسلوب يتوافق مع متطلبات تطوير الأمن السيبراني فهو يتطلب في البداية الى جهد ذاتي يتعلق في تطوير امكانيات الدولة وعلى المستويين الرسمي وغير الرسمي، لان التهديدات السيبرانية لا تنحصر عند فرد او مؤسسة فالجميع معرض لها مما يتطلب ان يكون استعداد شامل لدى الجميع، كما ان ذلك الامر لا يتطلب على توفير البنى التحتية فقط، انما يكون اوسع من ذلك عندما عملت على دعم الابتكارات في مجال الحد من الهجمات الالكترونية وتوسعت ايضاً عندما اشارت الى تعزيز التعاون والتنسيق مع الدول والمؤسسات.

وعليه فان نجاح الاهداف التي سعت اليها الحكومة البلجيكية يعتمد في الاساس على اليات انفاذها من قبل المؤسسات التي سيتم تناولها.

خامساً: اليات انفاذ السياسيات العامة في مملكة بلجيكا.

لقد استندت بلجيكا بعملها في مجال الأمن السيبراني كما موضح انفاً من خلال مستويين سياسات واليات تنفيذ. فعلى المستوى الاول اعتمدت على قوانين وسياسيات على مستوى الاتحاد الاوربي وسياسات على المستوى الوطني، فضلاً عن المجال التنفيذي هو الاخر شهد مؤسسات انفاذ على مستوى الاتحاد ومؤسسات على المستوى المحلي، الا ان ما يهمنا في هذه الجزئية من البحث التعرف على مؤسسات الانفاذ في دولة بلجيكا. يمكن تناولها على النحو الاتي:

١- المركز الوطني للامن السيبراني البلجيكي (CCB)

السلطة الوطنية المسؤولة عن الأمن السيبراني في بلجيكا. يعمل بشكل مركزي ويكون تابع الى وزارة الداخلية، لكنه يخضع بشكل مباشر تحت سلطة رئيس الوزراء(Jøsang 2018, 500) ، يمكن ايجاز اهم مهامه على النحو الاتي:

١- **الرقابة:** تتمثل عملية الرقابة في متابعة مستمرة للفضاء السيبراني من اجل رصد التهديدات السيبرانية والتحديات التي تواجه العمل، فضلاً عن متابعة الالتزامات الدولية والمقترحات الوطنية. كما يعمل المركز بدور مهم في الكشف والتنبيه من خلال عملية الرقابة ويكون ذلك بالتعاون مع فريق الاستجابة لحالات الطوارئ الحاسوبية عبر مراقبة وتحليل التهديدات، كما انه عزز من عملية الرقابة والابلاغ عن التهديدات السيبرانية، اذ عمل على انشاء موقع رسمي (CERT.be) يعمل باستمرار على استلام الرسائل والتبليغات من الافراد والمؤسسات عن الخروقات الالكترونية (Cybersecurity Strategy Belgium 2.0 2021,34).

٢- **الاشراف:** هذا الدور يتمثل في الإشراف على تنفيذ سياسة الأمن السيبراني البلجيكية بالكامل وكذلك في اصدار الاجراءات والتقارير والتوصيات حول طبيعة المخاطر وسبل مواجهتها. ويقوم بأعداد الارشادات حول طبيعة سلامة المعلومات، فضلاً عن إعلام وتوعية المستخدمين بشأن أنظمة المعلومات والاتصالات(Cybercrime 2018) .

٣- **التنسيق:** يتركز عمل المركز على انشاء خلية مشتركة من قبل المؤسسات الرسمية وغير الرسمية من اجل الحفاظ على سلامة مؤسساتها من الاختراقات الالكترونية وفقاً لنهج متكامل ومركزي، هذا التعاون والتنسيق لا ينصب على المستوى الوطني فقط؛ انما يمتد الى مستوى الاتحاد الاوربي والدول، بمختلف المجالات من بينها تنسيق التمثيل البلجيكي في المنتديات الدولية للأمن السيبراني، فضلاً عن صياغة المقترحات للتكييف مع الإطار التنظيمي للامن السيبراني على المستويات المحلية

والوطنية والدولية (Fagan 2023, 447). بمعنى اخر يقوم بتمثيل الدولة في المنتديات الدولية للأمن السيبراني، ومتابعة الالتزامات الدولية واقتراح الموقف الوطني في هذا المجال، بهدف اتخاذ إجراءات خارجية متماسكة بالتشاور مع وزارة الخارجية والأمن العام ووزارة الدفاع. فضلاً عن انه يعمل على تقييم وإصدار الشهادات الأمنية لانظمة المعلومات والاتصالات ويقترح على المؤسسات الاوربية اصدار الشهادات ووضع العلامات على المنتجات والخدمات من اجل ترصين كفاءة المؤسسات على مواجهة التهديدات وزيادة الثقة بها Cybersecurity Strategy Belgium 2.0 (2021,34).

٤- **المعالجة:** تتمثل في مواجهة أي خرق الكتروني قبل وبعد حدوثه من خلال اخذ الاحتياطات التامة على معالجته، وهذه المعالجة تكون اما بشكل مباشر من خلال ادواته الملتصقة في هيكله الاداري او بشكل غير مباشر من خلال البرامج التي يقوم على اعدادها من اجل تطوير مهارات الكيانات العامة والخاصة في مجال الأمن السيبراني. كما يقوم بنشر المبادئ التوجيهية ومعايير السلامة للحد من الهجمات السيبرانية (ICT Policy 2021, 447).

ان عمل الهيئة الوطنية تجسد في جملة من الوظائف التي بدأت من اجراءات الرقابة وانتهاءً بالمعالجات للخروقات التي تستهدف الافراد والمؤسسات بهذه الكيفية في العمل حاول صانع القرار البلجيكي ان يجد ارضية عمل ترتقي الى المؤسساتية؛ عندما جعل الهيئة الوطنية المنسق والموجه العام لاجراءات الأمن السيبراني؛ مع ربط كل هذا العمل مع مؤسسات وطنية مثل (المركز الوطني للأزمات) ومؤسسات الاتحاد الاوربي المسؤولة عن الأمن السيبراني.

٢- المركز الوطني للأزمات (NCCN)

يتولى المركز الوطني للأزمات التابع الى وزارة الداخلية، مهمة التنسيق والتعاون عند حدوث الازمات الكبيرة مع المركز الوطني والشرطة الفيدرالية البلجيكية، وكذلك مع الجيش، فضلاً عن التعاون مع القطاع الخاص والعام من اجل ايجاد معالجة مشتركة للهجمات السيبرانية، هذه المعالجة تتجسد في وضع خطة الطوارئ الإلكترونية على المستوى الوطني (Maniscalco and Rosato 2019).

لذا فان طريقة تفعيل عمل المركز الوطني للاستجابة يحصل عندما يكون هناك تهديد للامن الوطني سواء اكان هناك تهديد طارئ ام يتطلب الى اعداد العدة في مواجهته مستقبلاً، هذا الدور لا يقتصر على المستوى الوطني فقط، انما يمتد الى المستوى الدولي، اذ يقوم بالتنسيق وتبادل المعلومات مع المؤسسات الدولية مثل المؤسسات الاوربية المتعلقة في امن المعلومات والشبكات، وكذلك بقية دول العالم ويكون عمله في اوقات الطوارئ وفي الحالات الاعتيادية التي تتعلق في تدريب واجراء المحاكاة المستمرة في

التعامل مع التهديدات، ويقوم ايضاً بنشاطات التوعية بالمخاطر السيبرانية والتثقيف عليها(Willems 2019,176).

ان النظر الى عمل المركز نجده يمتاز بعمل مؤسساتي شامل بهذه الصيغة سيكون له القدرة والامكانية على معالجة التحديات من خلال تأسيس خلية عمل مشتركة بين المؤسسات المعنية على موجهة تحديات الأمن السيبراني.

٣- الشرطة (police)

تتحمل الشرطة هي الاخرى، مسؤولية مواجهة التهديدات السيبرانية في بلجيكا. وتعمل على مستويين هي:

- المستوى الفيدرالي: تقوم بهذه المهمة وحدة الجرائم الحاسوبية التابعة الى الشرطة الفيدرالية البلجيكية مهمتها التحقيق في الجرائم المتعلقة بالبيانات الالكترونية على المستوى الوطني (McKeown and Shefet 2023,162). وفي الوقت ذاته تعمل من خلال المركز الوطني على التعاون مع المؤسسات الدولية مثل (INTERPOL- Europol) والدول ايضاً كنقطة اتصال وطنية مع النهج الدولي لمكافحة الجرائم الإلكترونية...
- المستوى المحلي: تعمل من خلال وحدات الجرائم الحاسوبية المحلية (RCCUs) التابعة الى الشرطة المحلية باعتبارها نقطة الاتصال الأولى للمواطنين والشركات والوكالات الحكومية، وتستعين بوحدة الجرائم الحاسوبية الفيدرالية (FCCU) Cybersecurity Strategy (Belgium 2.0 2021,34).

وعليه تتحمل كلتا الوحدتين مسؤولية التعامل القانوني مع جرائم تكنولوجيا المعلومات والاتصالات التي تواجه الافراد والمؤسسات مثل الاحتيال الاكتروني وسرقة الهوية والجرائم المالية والاختراقات الالكترونية، فضلاً عن تعقب تجارة البيانات المسروقة وشبكات القرصنة وهجمات الفدية وغيرها من خلال تقديم المساعدة المتخصصة بالتحقيقات في بيئة محوسبة والقيام بالتحليل الجنائي لمواد تكنولوجيا المعلومات والاتصالات (أجهزة الكمبيوتر والهواتف الذكية) للقضايا المتعلقة بالجرائم الالكترونية، فهي تقوم بجمع الأدلة الرقمية بهدف تعقب الجناة وتقديمهم إلى العدالة.

٤- النيابة العامة (Public prosecution)

تمارس النيابة العامة في بلجيكا دور التحقيقات في المخالفات المتعلقة بالجرائم الالكترونية؛ ويكون ذلك بالتعاون مع الشرطة الفيدرالية، ومن خلال تلك التحقيقات؛ تقوم بتقديم المتهمين الى المحاكم، ويكون العمل في النيابة العامة في مجال الأمن السيبراني على مستويين وهي:

المستوى الفيدرالي: يقصد به الادعاء العام الذي يكون موجود في العاصمة البلجيكية بروكسل؛ يتم العمل من خلال تأسيس وحدة سيبرانية تضم قضاة فيدراليين؛ متخصصون بالتحقيق في الجرائم السيبرانية؛ ذات البعد الدولي التي ترتكبها شبكات الجريمة المنظمة؛ باستخدام تقنيات متقدمة، والتهديدات التي تطال البنية التحتية لتكنولوجيا المعلومات والاتصالات الحيوية. ويتولى المدعي العام الفيدرالي مهمة تعزيز التعاون الدولي مع مكتب المدعي العام في (EUROJUST) ، و"شبكة الجرائم السيبرانية القضائية الأوروبية" في سبيل جعل العمل اكثر شمولية وقدرة على معالجة المخالفات Cybersecurity Strategy Belgium) 2.0 2021,34).

المستوى المحلي: يقصد به المدعي العام الذي يكون على مستوى الاقاليم، ففي كل منطقة قضائية تكون تحت إشراف مدعي عام مختص في التحقيق بالجرائم الالكترونية، تتلخص مهامه في رصد المخالفات الالكترونية بعد ذلك يحيلها الى المحكمة من اجل التحقيق فيها(Ishikawa &Kryvoi 2023, 121).

وبذلك فان المدعي العام في كلى المستويين يعمل حلقة وصل بين المجتمع والجهات الرسمية والدولة والمجتمع الدولي في سبيل الحد من مخاطر التهديدات السيبرانية.

يتضح من ذلك ان الحكومة البلجيكية اوجدت طريقة لأنفاذ سياساتها السيبرانية من خلال تطبيقها بشكل واضح ومحدث، يعتمد على اسلوب وقائي وعلاجي في نفس، من خلال عمل مؤسساتها يقوم على اعداد العدة المسبقة في مواجهة التهديدات السيبرانية.

سادساً: مستقبل السياسات العامة للأمن السيبراني في بلجيكا.

ان التطرق الى موضوع المستقبل بشكلٍ عام والسياسات العامة للأمن السيبراني في بلجيكا بشكلٍ خاص، يتطلب طرح ثلاثة مشاهد بين التطور والتراجع والبقاء على ما هو عليه، مع افتراض في كل مشهد عن الاتجاه الذي سيكون عليه في ظل المعطيات الموجودة على البيئة الرقمية. يمكن تناولها على النحو الاتي:

١- **مشهد تطور السياسات العامة السيبرانية:** ينطلق هذا المشهد من تصور مفاده ان السياسات السيبرانية للحكومة البلجيكية، ستشهد تطوراً ملحوظاً في اجراءات مواجهة التهديدات السيبرانية، ويستند في ذلك الى جملة من المعطيات التي تقوم عليها البنية الرقمية في بلجيكا. ان هذا التطور المحتمل الذي تصل اليه السياسات العامة للأمن السيبراني هو في الاساس نتيجة حتمية لهذا النوع من السياسات، لان عملها يكون منصب في بيئة صراع مستمرة لا تتحدد وفقاً للأطر الزمانية والمكانية التي تنعدم فيها محددات الصراع، فضلاً عما يدور في الفضاء السيبراني من الغموض وعدم الوضوح، لاسيما فيما يتعلق بمجهولية المعتدي من حيث الهوية والمكان والزمان، هذا الامر يصل الى عدم معرفة المعتدي ان كان انساناً او برنامجاً او ريبورت الياً الذي اوجده الذكاء الاصطناعي.

وبذلك يكون مشهد التطور للامن السيبراني في بلجيكا هو البحث بشكل مستمر عن نقاط الضعف التي تشتمل عليها اجراءات الحماية، من خلال المتابعة والمراقبة المتتالية من اجل اصلاح المشاكل التي تتعرض لها شبكة الحماية، مع اجراء تحديث وتطوير مستمر للبنية التشريعية والتحتية المتمثلة في العمل على تطوير الانظمة والبرامج الالكترونية من خلال اعادة برمجتها وتحديثها بشكل مستمر، لكي تكون قادرة على مواجهة الهجمات السيبرانية(**McDermott 2010, 209**) .

وكذلك فان مشهد التطور وما يرمو اليه يفترض ان الحكومة البلجيكية تعزز من اهمية بث الوعي لدى افراد المجتمع، لتعريفهم بشكل اكبر مدى خطورة الهجمات السيبرانية على امنهم الخاص المتعلق بخصوصياتهم المالية والاجتماعية وامن الدولة بشكل عام. كما انه من المحتمل ان يكون هناك زيادة في حجم الاستثمارات في مجال الأمن السيبراني، وهذا الاستثمار يكون على مستويين؛ الاول في مجال التقنية من اجهزة وبرامج وغيرها؛ والثاني في مجال بناء القدرات البشرية القادرة على استخدام التقنية في مواجهة الهجمات السيبرانية **(Karathanasis 2024, 44)** .ومع ذلك فان مشهد التطور لا يقف عند ذلك انما يكون في بناء اطار مؤسساتي يأخذ ثلاثة مستويات. الاول على المستوى الداخلي؛ والذي يتمثل في ايجاد تعاون وتنسيق على مستوى عالي بين الحكومة والشركات والافراد. والثاني على المستوى الاقليمي؛ المتمثل في زيادة التعاون مع مؤسسات الاتحاد الاوربي وحلف الناتو، من اجل ان تكون هناك سياسة موحدة تقوم على مواجهة التهديدات السيبرانية. والثالث على المستوى الدولي، والذي يكون عن طريق التعاون مع الامم المتحدة والدول المتقدمة في مجال الأمن السيبراني، وبذلك ستكون سياسة الأمن السيبراني قد حققت تطوراً ملموساً قادراً على الاستجابة مع تطور التحديات التي يفرضها الفضاء السيبراني (OECD 2022, 49) .

١- **مشهد البقاء على ما هو عليه:** يفترض في هذا المشهد بقاء اداء سياسات الأمن السيبراني في بلجيكا على نفس المستوى في مواجهة التهديدات السيبرانية، بمعنى تكون السياسة ما بين الشد والجذب في عملية صد الهجمات السيبرانية. ومع دراسة الحالة البلجيكية وجد هناك سياسات واليات انفاذ عملت على تأسيس اطر وقائية دفاعية تقوم على تأمين البيئة الالكترونية، الا انها رغم كل الامكانيات التي امتلكتها فقد تعرضت في بعض الاحيان الى الاختراقات السيبرانية وصدت البعض الاخر.

بشكلٍ عام تعد بلجيكا واحدة من اكثر الدول تعرضاً للهجمات السيبرانية كونها تمثل مقر اقامة حلف الناتو والاتحاد الاوربي ما يجعلها هدفاً مستهدفاً بشكل كبير من اجل اختراق بياناتها او تخريب بنيتها التحتية في سبيل اعاقة وتخريب اجهزت الناتو والاتحاد الاوربي. لذا كان استعداد الحكومة لهذا التهديد يقوم على اعداد بنية سيبرانية تضمن توفير الانظمة والبرامج والكوادر الماهرة وتخصيص الموارد لسد متطلبات الأمن السيبراني(Gérard &Gérard 2020 , 8) ، فضلاً عن وجود مظلة امن سيبرانية

اوروبية اشتملت على جملة من المؤسسات المسؤولة عن توفير الحماية السيبرانية مثل الوكالة الاوربية للامن السيبراني التي تقوم على تعزيز الأمن السيبراني في الاتحاد ومركز الكفاءة السيبراني الذي يعمل على تعزيز التعاون وتمويل المشاريع البحثية ووحدة التعاون السيبراني التي تقوم على تعزيز التعاون بين دول الاتحاد ومكتب الاتحاد الاوربي للمعلومات الاستخباراتية المسؤول عن تحليل البيانات وتقديم تقارير استخباراتية. ولكن يبقى السؤال في هذا هل ان هذه السياسات تمكنت من مواكبة التطورات على الساحة السيبرانية (Kindt 2013, 328) . فمن خلال بحثنا انفاً وجد هناك مسعى كبير من قبل الحكومة السيبرانية والاتحاد السيبراني على مواجهتها. مع ذلك بقاء الحال عما هو عليه من دون اجراء تطور مستمر يتعاطى مع التحديثات التي تقوم بها الهجمات السيبرانية. لا يمكن ان تشهد سياسة الأمن السيبراني تطوراً ملحوظاً سوى بقاءها على مستواها في مواجهة الهجمات السيبرانية.

٢- **مشهد التراجع:** يرتبط هذا المشهد بمعادلة الأمن السيبراني الذي تقوم على وجود تسابق مستمر بين مقومات المواجهة للدولة وبين تطور وتنوع طرق المهاجمة، فهذا المشهد يفترض ان عمليات التطور في المواجهة من قبل الحكومة البلجيكية، اذا لم تكن متوازية مع سباق المواجهة فان السياسة العامة للامن السيبراني ستكون في حالة تراجع وعدم القدرة على الصمود امام تحديات الأمن السيبراني، هذا المشهد يكون حاضراً في حالة تراجع الحكومة البلجيكية عن مواكبة تحديات السيبرانية نتيجة عدم اجراء التحديثات المستمرة للسياسات التي تصنها، ويصاحب ذلك تراجع اداء مؤسسات انفاذها في المواجهة، هذا التراجع يتجسد في عدم اعطاء الاهمية والاولوية للقطاع الخاص افراداً ومؤسسات على المشاركة في المواجهة، فالفرد يمثل الحلقة الاضعف من حلقات الأمن السيبراني، فاذا لم تلتزم الحكومة في تركيز جهودها على تنفيذ التزاماتها التي وضعتها ضمن اهدافها الرئيسة في سياساتها فان ذلك سيمثل ثغرة امام قدراتها في المواجهة (Subrahmanian and others 2015, 109) ، كما ان عالم التقنية الرقمية اعطى لشركات القطاع الخاص المالك لها من حيت الانتاج والتسويق ولكن في نفس الوقت تكون بحاجة الى دعم مستمر من قبل الحكومة ففي حالة تقاعسها عن ذلك يؤثر سلباً على الاداء، ومع ذلك فان بلجيكا لديها التزام عضوي مع الاتحاد الاوربي فان تراجع الحكومة عن التركيز على التعاون والتنسيق بين مؤسسات الاتحاد سيشكل تحدياً كبراً ، (OECD 2022, 49)) فضلاً عن ذلك فان الاتحاد الاوربي والناتو في ظل التحديات الذي يواجهانهما جراء حرب اوكرانيا ووصول دونالد ترامب الى سدة الحكم في الولايات المتحدة الامريكية الذي يسعى الى تخفيض الدعم الى اوروبا، يمكن ان يشهد تراجعاً في الاداء السيبراني مع تصاعد الهجمات السيبرانية ما يؤثر على تراجع سياسات الأمن السيبراني في بلجيكا(International Monetary Fund 2023, 17).

يتضح من ذلك ان المشاهد الثلاثة للامن السيبراني في بلجيكا قد اخذ كل واحد منحاً خاصاً به، وذلك بالاستناد على جملة من المعطيات، ومع ذلك فان ما تحمله اوروبا من اهمية وتقدم تكنلوجي وسياسي واجتماعي واقتصادي فان مشهد التطور يكون اقرب الى الواقع.

الخاتمة:

في الختام توصل البحث الى ان مملكة بلجيكا بمعية الاتحاد الاوربي ادركت منذ بداية التغيير الذي احدثته التقنية في مفهوم الأمن الذي اخذ يعبر عن الاجراءات التي تتخذها الدول في سبيل حماية الانظمة والبرامج والشبكات الالكترونية من الهجمات السيبرانية، لذا عملت من خلال مؤسساتها التشريعية والتنفيذية والقضائية وبالمشاركة مع مؤسسات الاتحاد الاوربي على صنع سياسات عامة تقوم على التأسيس لبنية تحتية قادرة على مواجهة التهديدات السيبرانية، لكن مع ذلك واجهة هذه السياسات جملة من التحديات مما دفع بها الى اجراء تحديث مستمر لسياساتها المتمثلة في القوانين والاستراتيجيات، وما نتج عنها من تعدد وتنوع مؤسسي للحد من الهجمات السيبرانية.

كما ان هذا الادراك المبكر لحجم المخاطر السيبرانية عمل على جعل صناعة السياسة العامة، تكون من قبل مجلس الأمن القومي الذي يمثل اعلى مؤسسات الدولة الأمنية في مملكة بلجيكا ومسؤوليته تفعل عندما يكون هناك خطر محدق يهدد العمق الأمني في البلاد، لأنه وفقاً للحسابات الأمنية فان التهديدات التي تفرضها الهجمات السيبرانية تكون شاملة وواسعة تصل الى مؤسسات التشريع والتنفيذ والقضاء ومؤسسات القطاع الخاص، وحتى الافراد لن يكونوا في مأمن ما يجعل قرارات وموارد البلاد في خطر كبير امام هذا التحدي.

وفي ظل هذه المخاطر التي تفرضها السيبرانية وطريقة الهجمات المتبعة فيها، تكون بلجيكا اكثر تعرضاً لها من الدول الاخرى بحكم اتخاذها مقراً للاتحاد الاوربي، فضلاً عن فعالية انشطتها التجارية وتركيز الحكومة جهودها على نقل انشطتها من الاعمال التقليدية الى اعمال قائمة على اسس الحوكمة في جميع انشطتها التجارية والسياسية والاجتماعية وغيرها، جعل منها تكون محل للهجمات اكثر من غيرها. ونتيجة الى تلك الاسباب وجد هناك تعدد في صنع السياسات العامة؛ ما بين سياسات اقليمية يتخذها الاتحاد الاوربي، ووطنية تصنعها الحكومة بالاستناد الى سياسات الاتحاد؛ وفي كلتا المستويين وجد هناك تعدد وتحديث مستمر لها. وفي الوقت ذاته عند الملاحظة ان انفاذ السياسات العامة في بلجيكا اتخذت الحكومة الاسلوب المركزي في كثير من الاحيان لا سيما مع الهجمات الخارجية؛ وهو ما يختلف مع الشكل الفيدرالي للدولة الذي يقوم على توزيع الصلاحيات، كان السبب في ذلك هو حجم المخاطر الكبيرة الذي تمثلها التهديدات السيبرانية؛ التي تميزت بالسرعة وعدم التنبئ بها؛ وطبيعة الاضرار الكبيرة التي تسببها؛ تتطلب ذلك من الحكومة البلجيكية ان يكون هناك سرعة في الاستجابة عند التعرض للهجوم

وامكانيات مادية كبيرة تحتاج اليها المؤسسات القائمة على توفير الأمن السيبراني؛ وتقنيات متطورة من انظمة وبرامج وكوادر بشرية متدربة تملك الخبرة اللازمة في مواجهة الهجمات السيبرانية، فضلاً عن هذا النوع من الأمن يتطلب تمثيل دولي موحد للدولة يتعاطى مع القرارات والتوجيهات التي تتخذ على المستوى الدولي. لكن العمل المركز ليس مطلقاً في بلجيكا فقد اتبعت اللامركزية في بعض الاحيان، اشتملت على الخروقات التي تقع على الافراد والمؤسسات الصغيرة، هذا العمل كان حكراً على المؤسسات الأمنية التقليدية والقضائية من اجل فرض العقوبات على المخالفين.

واخيراً شكل الأمن السيبراني تحدياً كبيراً ومستمراً وامكانية للتطور في ان واحد امام سياسة الحكومة البلجيكية، لأنه يحتاج الى حلول مبتكرة وقادرة على التعاطي مع تهديدات الفضاء السيبراني المتجددة.

الاستنتاجات:

١- اصبحت اهداف السياسة العامة للأمن في الفضاء السيبراني تقوم على حماية البرامج والانظمة الرقمية من الهجمات السيبرانية؛ بعد ان كان الأمن يتمثل في حماية موجودات الدولة، مما اضاف متغير جديد على عناصر سيادة الدولة؛ وهو الحفاظ على المعلومات البيانية. وبذلك اصبحت الخروقات التي تقوم بها الهجمات السيبرانية هو خرق لسيادة الدولة في بلجيكا او بالاحرى ان سيادة الدولة في ظل السيبرانية؛ ما عادة كالسابق لان السيبرانية تمكن الافراد والمؤسسات والدول من اختراق خصوصيات الدول الاخرى، لذا سنكون امام عالم مفتوح لا تحدده اطر جغرافية يفرضها الفضاء السيبراني.

٢- اعتمدت الحكومة البلجيكية على مراحل صنع السياسات العامة التي تمثلت في رسم الاطار العام للسياسة حول طبيعة المشاكل، وانتقلت بعد ذلك الى صنع السياسة العامة؛ وذلك بعد اخذ التصور العام لحجم التحديات السيبرانية؛ وطرق مواجهتها بأسلوب يتماشى مع حجم المخاطر؛ ووضعت ادوات انفاذ تتناسب مع طبيعة الجرائم السيبرانية التي تتخذ اشكالات وممارسات مختلفة ومتعددة الانماط، من خلال جعلها مؤسسات تمتلك الامكانيات الكافية على مواجهته، ولم تكتفي عند ذلك انما اجرت عملية تقييم مستمرة لطبيعة الاداء على المستويين النظري والعملي، ينتج عن هذه العملية اجراءات تقويمية مستمرة تعمل على تصحيح الاخطاء او العمل على تحديث السياسات تماشياً مع تطور التحديات السيبرانية.

٣- اسهمت السياسة العامة للحكومة البلجيكية في جعل القطاع الخاص شريكاً اساسياً في مواجهة التهديدات السيبرانية، اذ فسحت المجال امام شركات القطاع الخاص على تطوير تقنيات الدفاع السيبراني وسبل مواجهته، وعمقت من حجم التعاون بينها وبين الشركات كما هو موضح في متن البحث، والسبب في ذلك يعود لان نسبة كبيرة من البنية التحتية من الانظمة والبرامج وغيرها

تكون مملوكة الى القطاع الخاص، هذا التعاون تجسد في تبادل الخبرات وتقديم الدعم من الحكومة ولاسيما في مجال الاستثمار في التقنية، وبهذه الكيفية اصبحت السياسة العامة الوطنية للحكومة البلجيكية تستند على ركيزتين اساسيتين الحكومة والقطاع الخاص.

٤- لقد عدت السياسة العامة في مملكة بلجيكا للأمن السيبراني ضرورة من ضرورات الدولة؛ وليس مجرد خيار او اجراء احترازي تسعى الدولة للخلاص منه، بمعنى اصبحت السيبرانية غاية تسعى اليها الحكومة وليس خيار يمكن ان تتجاهله، بسبب تزايد الاعتماد الكبير على التكنلوجيا في مختلف انشطتها؛ وما يترتب على ذلك من زيادة في مخاطرها الأمنية التي تحدث ضرراً في الافراد والمؤسسات، ما جعل من سياسات الحماية الرقمية استراتيجية اولية للحكومة والافراد والشركات في اتخاذ الاجراءات اللازمة المتمثلة في الموارد والتقنيات لمواجهة التهديدات.

٥- لقد عدت سياسة الحكومة البلجيكية الأمن السيبراني مسؤولية مشتركة لا تقتصر على الحلول التقنية فقط، انما مسؤولية تتطلب تعاوناً بين الافراد والحكومة والشركات والمؤسسات الربحية والبحثية والمجتمع الدولي، لان عملها لا يمكن حصره على حيز مكاني او زماني، ولا يمكن معرفة الطريقة التي يهاجم بها؛ وكذلك العنصر المستهدف، وفي نفس الوقت لا يمكن معرفة القائم بالاعمال الجرمية، ما تطلب الى وجود عمل مشترك يقوم به الجميع من اجل توفير الحماية الكافية للدولة.

٦- لقد امتازت السياسة العامة للامن السيبراني في مملكة بلجيكا بالمرونة والقابلية على التطبيق، كونها قابلية للتكيف مع البيئة السيبرانية التي تفرض تهديدات تتنوع وتختلف بين الحين والاخر؛ ما بين تهديدات سياسية واقتصادية واجتماعية؛ فمرة نجدها تتعامل مع حماية المؤسسات السياسية وما تتضمنه من قرارات مهمة في البلاد؛ ومرة نجدها تقوم على حماية المؤسسات المالية مصارف وبورصات وغيرها، وحماية خصوصيات الافراد من جهة اخرى. هذه المرونة لم تقتصر على ذلك انما مع التغيرات السريعة للتكنلوجيا؛ وما تفرضه من اجراءات جديدة تتطلب العمل بها، وكذلك مع التغيرات القانونية التي من الممكن ان تتعارض معها وعلى المستويين الدولي والمحلي.

٧- لقد حاولت السياسة العامة للامن السسبراني توفير اغلب المستلزمات التي تتطلبها مواجهة التهديدات السيبرانية، الا ان هذا التحدي لا يمكن مكافحته بشكل نهائي؛ لما يتمتع به من خصائص ديناميكية يصعب احتوائها بشكل مطلق وقاطع، فضلاً عن ذلك هناك تحديات لوجستية تتمثل اولها في التحدي المالي لان ميزانية الأمن السيبراني تكون في العادة مثقلة بالنفقات الكبيرة؛ نتيجة التكلفة العالية للتقنية المطلوبة من البرامج والانظمة في مواجهة المخاطر

السيبرانية، وتحدي صعوبة الحصول على التقنية بشكل مستمر بحيث يمكن مواكبة التطورات التي تمر عليها، فالتقنية السيبرانية قد تكون مصنعة من دول لا ترتبط بعلاقات وطيدة مع بلجيكا، او تحمل العداء لها مما يصعب الحصول عليها، وهذا الامر لا يستوقف عند الدول؛ انما حتى مع القطاع الخاص ولا سيما بعد ان اصبح له دوراً كبيراً في انتاجها مما يصعب في بعض الاحيان؛ التعاون بين الحكومة البلجيكية وهذه الشركات، وايضاً لا تقف التحديات هنا انما تصل الى التناقض في بعض الاحيان ما بين سياسية الاتحاد الاوربي والسياسة الوطنية للحكومة البلجيكية.

المصادر باللغة الانكليزية:

1. Akinwale, Akeem Ayofe & Afolayan ,Gbenga Emmanuel. 2017 . Global Perspectives on Development Administration and Cultural Change. IGI Global . United States .
2. Armstrong, Jonathan. 2012. Mark Rhys-Jones ،Daniel Dresner. Managing Risk: Technology and Communications. Taylor & Francis Group. New York.
3. Baezner, Marie and Cordey, Sean. 2022.Influence operations and other conflict trends. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
4. Bonfanti, Matteo E. 2022. Artificial intelligence and the offense–defense balance in cyber security. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
5. Brown, Mary Maureen & Garson, G. 2013. David. Public Information Management and E-government: Policy and Issues. Information Science Reference .USA.
6. Cavelty ,Myriam Dunn and Wenger, Andrea. 2022. cyber security politice socio-technological trans formstion and political frag mentation. Routledge. New York.
7. Cavelty, Myriam Dunn and Wenger, Andreas. 2022. uncertainty and political fragmentation. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
8. Chané ,Anna-Luise and others . 2020.The European Union and Human Rights: Law and Policy. First Edition published. Oxford University Press. New York ..
9. Couriel , Deborah Housen. 2025. Cybersecurity and national security: integrating new challenges. A Research Agenda for Cybersecurity Law and Policy. The Editors and Contributors Severally. Edward Elgar Publishing Limited. UK..
10. Couriel , Deborah Housen. 2025. Cybersecurity and national security: integrating new challenges. A Research Agenda for Cybersecurity Law and Policy. The Editors and Contributors Severally. Edward Elgar Publishing Limited. UK.
11. Cybercrime. Belgium. 2018. file:///C:/Users/Administrator/Desktop
12. Cybersecurity Strategy Belgium 2.0 2021-2025. 2021. Centre for Cybersecurity Belgium. Brussels. May.

13. Easttom, Chuck. 2021. Modern Cryptography: Applied Mathematics for Encryption and Information Security. Springer International Publishing. USA.
14. Eriksson,Johan and Giampiero, Giacomello.2022.Cyberspace in space:Fragmentation.vulnerability. and uncertainty. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
15. Fagan, Peter. 2023. The Business of Cyber ,Why You Should Question What Your Security Team Are Telling You. Peter Fagan.
16. Fang ,Binxing. 2018. Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace. Science Press and Springer Nature Pte Ltd. Singapore.
17. Felkner, Anna and others. 2021. Cybersecurity Research Analysis Report for Europe and Japan Cybersecurity and Privacy Dialogue Between Europe and Japan. Springer Nature Switzerland AG.
18. Flkner, Anaa And others . 2021. Cybersecurit Researcg Analysis Report forbEurope and Japan. The Editor(s) (if applicable) and The Authors). under exclusive license to Springer Nature Switzerland AG.
19. Francisco, Jose Ruiz and others. 2021. Cybersecurity Research Analysis Report for Europe and Japan: Cybersecurity and Privacy Dialogue Between Europe and Japan. Springer International Publishing Switzerland.
20. Geers, Kenneth. 2011.Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence. Estonia.
21. Gérard Cliquet&Gérard Cliquet. Location-Based Marketing: Geomarketing and Geolocation. Wiley & Sons. Incorporated. Hoboken . 2020.
22. Goetry, Bram and others. 2024. The Legal 500 Country Comparative Guides Belgium Data Protection & Cybersecurity. Legalease Ltd. UK.
23. Group of authors. 2021. ICT Policy. Research. and Innovation: Perspectives and Prospects for EU-US Collaboration. Wiley & Sons. Incorporated. Hoboken . .
24. Gruschka, Nils. 2018. Secure IT Systems : 23rd Nordic Conference. NordSec 2018. Oslo. Norway. November 28-30. Proceedings. Springer International Publishing.
25. Guitton ,Clement and others . 2015. Cybersecurity at Stake: Monitoring Threats. Managing Risks and Defensive Measures. Jean-Loup Richet. Cybersecurity Policies and Strategies for Cyberwarfare Prevention. IGI Global. USA.
26. Guitton ,Clement and others . 2015. Cybersecurity at Stake: Monitoring Threats. Managing Risks and Defensive Measures. Jean-Loup Richet. Cybersecurity Policies and Strategies for Cyberwarfare Prevention. IGI Global. USA.
27. ICT Policy. 2021. Research. and Innovation: Perspectives and Prospects for EU-US. Svetlana Klessova. 2021 The Institute of Electrical and Electronics Engineers. New York.
28. International Monetary Fund . 2023. Monetary and Capital Markets Department. Financial Sector Assessment Program-Financial System Stability Assessment. International Monetary Fund. Washington.
29. Ishikawa, Tomoko. Kryvoi, Yarik.2023. Public and Private Governance of Cybersecurity: Challenges and Potential. Cambridge University Press. UK.
30. Jakobs, Kai. 2009.Information Communication Technology Standardization for E-business Sectors: Integrating Supply and Demand Factors. Information Science Reference. London.

31. Jøsang, Audun. 2018, 17th European Conference on Cyber Warfare and Security ECCWS V2. Academic Conferences Limited.
32. Karathanasis, Theodoros. 2024. Cybersecurity and EU Law: Adopting the Network and Information Security Directive. Taylor & Francis. New York.
33. Karyda ,Maria. 2017. Fostering Information Security Culture In Organizations: A Research Agenda. Association for Information Systems AIS Electronic Library (AISeL).
34. Kindt , Els J. 2013. Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Springer Netherlands. New York.
35. Kuerbis ,Brenden and other. 2022.Understanding transnational cyber attribution: Moving from "whodunit" to who did it. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
36. Langella, Alessandra and others. 2023. GDPR Requirements for Biobanking Activities Across Europe. Editors: Valentina Colcelli. Roberto Cippitani. Christoph Brochhausen-Delius. Rainer Arnold. Springer International Publishing. Cham. Switzerland.
37. Maniscalco ،Maria Luisa and Rosato, Valeria. 2019. Preventing Radicalisation and Terrorism in Europe: A Comparative Analysis of Policies . Cambridge Scholars Publishing.UK.
38. Mayer, Sebastian. 2023. Research Handbook on NATO. Edward Elgar Publishing. Cheltenham.
39. McDermott, Rose . 2010. Decision Making Under Uncertainty. Proceedings of a workshop on deterring cyberattacks Informing Strategies and Developing Options for U.S. Policy. the National Academy of Sciences.
40. McKeown, Margaret M. and Shefet, Dan. 2023. Hate Speech. A Comparative Analysis of the United States and Europe. Regulating Cyber echnologies Privacy vs Security. World Scientific Publishing Europe Ltd. Singapore .
41. Newton, Michael A. 2010. Terrorism: International Case Law Reporter . Oxford University Press. Incorporate.New York. Volume II.
42. Nunes, Sérgio. 2023. Defining Cyber Risk Management Objectives. Regulating Cyber echnologies Privacy vs Security. World Scientific Publishing Europe Ltd. Singapore ..
43. OECD. 2022. OECD Economic Surveys: Belgium. OECD Publishing.
44. O'Neill, Maria & Swinton, 2013. Ken. New Challenges for the EU Internal Security Strategy. First Published. Cambridge Scholars Publishing. Newcastle upon Tyne.
45. O'Neill, Maria & Swinton, 2013. Ken. New Challenges for the EU Internal Security Strategy. First Published. Cambridge Scholars Publishing. Newcastle upon Tyne.
46. Paulus, Alexandra. 2024. Building Bridges in Cyber Diplomacy: How Brazil Shaped Global Cyber Norms. Springer Nature Switzerland. Cham. Switzerland .
47. Rondelez, Rafael. 2018. Governing Cyber Security through Networks: An Analysis of Cyber Security Coordination in Belgium. International Journal of Cyber Criminology. . Vol. 12(1).
48. Santos ,Larissa Galdino de Magalhães. 2024.Dynamic Capabilities in the Public Sector to Deal with GovTech. Electronic Government. Group of authors. Springer Nature Switzerland. Cham. Switzerland .

49. Steed ,Danny. 2022. Disrupting the second oldest profession: The impact of cyber on intelligence. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
50. Steiger, Stefan. 2022.Cyber securities and cyber security politics: Understanding different logics of German cyber security policies. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
51. Subrahmanian , V.S. and others. 2015.The Global Cyber-Vulnerability Report. Springer International Publishing. Switzerland. pp109.
52. Summers ،Sarah . 2014 . Christian Schwarzenegger ،Gian Ege ،Finlay Young The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society. Bloomsbury Publishing. London.
53. Svard, Proscovia & Joshi, Somya. 2015. Prerequisites to e-Government Development and Open Government: The Case of Three Municipalities. Cedem15: Proceedings of the International Conference for E-Democracy and Open Government. (Editors) Peter Parycek. Noella Edelmann. Donau-Universität Krems. Austria .
54. Tan ,Shamane. 2019. Cyber Risk Leaders: Global C-suite Insights Leadership & Influence in the cyber age . First published. MySecurity Media Pty Limited. Singapore.
55. Wenger, Andreas and Cavelty, Myriam Dunn. 2022. Index. Conclusion: The ambiguity of cyber security politics in the context of multidimensional uncertainty. Myriam Dunn Cavelty and Andreas Wenger. Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. New York. NY: Routledge.
56. Willems, Eddy. 2019. Cyberdanger: Understanding and Guarding Against Cybercrime. Springer Nature Switzerland AG.