Hybrid Warfare on Estonia 2007: A Foundational Model for National Resilience in the Face of Cyber Threats

Basil Muhammad Zeina*
Dr. Nour eddin Hermez**
Dr. Duraid Al-Essa***

(Received 19 / 10 / 2025. Accepted 28 / 4 / 2026)

□ ABSTRACT □

The hybrid warfare waged against Estonia in April 2007 represented a paradigm for modern conflicts in the 21st century, serving as a real-world laboratory for testing the effectiveness of unconventional strategies that blend electronic, informational, civil unrest, and political-economic pressure tools. This study aims to analyze this war as a comprehensive case study, seeking to extract the strategic lessons that countries, particularly small and medium-sized ones, can benefit from in building their national resilience against hybrid threats. The study relies on the case study methodology by analyzing the historical and political context of the attack, deconstructing its various dimensions (electronic, informational, civil, and diplomatic), and evaluating Estonia's response at national and international levels. The study concludes that the learned lessons revolve around several key pillars, most notably: the necessity of integrating cybersecurity into the core of national security, building effective public-private partnerships, enhancing societal resilience in the face of information warfare, and the importance of international cooperation and alliances in deterring these threats. This study contributes to Arabic literature on cybersecurity and hybrid warfare, providing a practical analytical framework that researchers and decision-makers can utilize.

The research concludes that successfully countering hybrid warfare relies less on military strength and more on comprehensive institutional and societal resilience, coupled with the imperative to develop international cooperation frameworks to address the legal and security loopholes exploited by such conflicts.

Keywords: Hybrid Warfare, Estonia, National Resilience, Cybersecurity, Cyber Attack.

Copyright **:**Latakia University journal (formerly tishreen) -Syria, The authors retain the copyright under a CC BY-NC-SA 04

* **PhD student- Department of Economics and Planning - Faculty of Economics - Lattakia University** basel.zaine@latakia-univ.edu.sy.

** **Professor - Department of Economics and Planning - Faculty of Economics - Lattakia University** Noureddin.hermez@latakia-univ.edu.sy.

*** **Associate Professor - Department of Economics and Planning - Faculty of Economics - Lattakia University** Duraed.al-issa@latakia-univ.edu.sy.

الحرب الهجينة على إستونيا 2007: نموذج تأسيسي للمرونة الوطنية في مواجهة التهديدات السيبرانية

باسل محمد زينه*

د. نور الدين هرمز**

د. دريد العيسى***

(تاريخ الإيداع 19 / 10 / 2025. قُبِل للنشر في 28 / 4 / 2026)

□ ملخّص □

شكلت الحرب الهجينة التي شُنت على إستونيا في نيسان 2007، نموذجاً للصراعات الحديثة في القرن الحادي والعشرين، حيث مثلت مختبراً حياً لمعرفة مدى فعالية استراتيجيات غير تقليدية تجمع بين الأدوات الإلكترونية والمعلوماتية والاضطرابات المدنية والضغوط السياسية والاقتصادية. تهدف هذه الدراسة إلى تحليل هذه الحرب بوصفها حالة دراسية شاملة، سعياً لاستخلاص الدروس الاستراتيجية التي يمكن أن تستفيد منها الدول، وخصوصاً الصغيرة والمتوسطة منها، في بناء مرونتها الوطنية في مواجهة التهديدات الهجينة. تعتمد الدراسة على منهج دراسة الحالة، من خلال تحليل السياق التاريخي والسياسي للهجوم، وتفكيك أبعاده المختلفة (الإلكتروني، المعلوماتي، المدني، والدبلوماسي)، وتقييم استجابة إستونيا على المستويات الوطنية والدولية. وتخلص الدراسة إلى أن الدروس المستفادة تتمحور حول عدة محاور أساسية، أبرزها: ضرورة دمج الأمن السيبراني في صميم الأمن القومي، وبناء شراكات فعالة بين القطاعين العام والخاص، وتعزيز المرونة المجتمعية في مواجهة الحرب المعلوماتية، وأهمية التعاون الدولي والتحالفات في ردع هذه التهديدات. تقدم هذه الدراسة إسهاماً في الأدبيات العربية المتعلقة بالأمن السيبراني والحرب الهجينة، مقدمةً إطاراً تحليلياً عملياً يمكن للباحثين وصناع القرار الاستفادة منه.

وتخلص الدراسة إلى أن نجاح مواجهة الحرب الهجينة لا يعتمد على القوة العسكرية بقدر ما يعتمد على مرونة مؤسسية ومجتمعية متكاملة، مع ضرورة تطوير أطر تعاون دولي لسد الثغرات القانونية والأمنية التي تستغلها هذه الحروب.

الكلمات المفتاحية: الحرب الهجينة، إستونيا، المرونة الوطنية، الأمن السيبراني، الهجوم الإلكتروني.

حقوق النشر : مجلة جامعة اللاذقية (تشرين سابقاً)- سورية، يحتفظ المؤلفون بحقوق النشر بموجب الترخيص CC BY-NC-SA 04

* **طالب دكتوراه- قسم الاقتصاد والتخطيط- كلية الاقتصاد- جامعة اللاذقية** basel.zaine@latakia-univ.edu.sy

** **أستاذ- قسم الاقتصاد والتخطيط- كلية الاقتصاد- جامعة اللاذقية** Noureddin.hermez@latakia-univ.edu.sy

*** **أستاذ مساعد - قسم الاقتصاد والتخطيط- كلية الاقتصاد- جامعة اللاذقية**
Duraed.al-issa@latakia-univ.edu.sy

مقدمة:

شكّل الهجوم المنسق الذي استهدف جمهورية إستونيا في ربيع عام 2007 منعطفاً تاريخياً في مفهوم الصراع الدولي. لم تكن المواجهة تقليدية بجنود ودبابات، بل كانت "حرباً هجينة" بامتياز، امتزجت فيها الأدوات العسكرية المحدودة مع هجمات إلكترونية ضخمة، وحملات معلوماتية مكثفة، واضطرابات مدنية موجهة، وضغوط دبلوماسية واقتصادية. حيث جسّد هذا الهجوم السمات الرئيسية للحرب الهجينة: الغموض، وإنكار المسؤولية، واستهداف النسيج الاجتماعي والدعائم الاقتصادية للدولة.

أما سبب اختيار هذه الحالة للدراسة فهو لأنها أول هجمة هجينة واسعة النطاق في العصر الرقمي، ما يجعلها "حالة مختبرية" غنية بالدروس. يهدف هذا البحث إلى تحليل هذه الحرب، سعياً لتحقيق عدة أهداف، أولاً: بناء إطار نظري لمفهوم الحرب الهجينة وأركانها. ثانياً: تحليل تفصيلي لهجوم 2007 بوصفه دراسة حالة. ثالثاً: استخلاص الدروس الاستراتيجية والتكتيكية على المستويات الوطنية والدولية. تعتمد المنهجية على تحليل دراسة الحالة، مستندة إلى المصادر الأولية (كالتقارير الرسمية وبيانات المسؤولين) والثانوية (كالأبحاث والتحليلات الأكاديمية).

ينقسم هذا البحث إلى ثلاثة فصول رئيسية: يتناول الفصل الأول الإطار النظري للحرب الهجينة، ويحلل الفصل الثاني حالة إستونيا، بينما يخصص الفصل الثالث لتحليل النتائج واستخلاص الدروس المستفادة.

الدراسات السابقة:

1- دراسة (**العاني، 2010**) بعنوان: "الحرب الإلكترونية: الهجوم على إستونيا أنموذجاً"، هدفت إلى التركيز على البُعد الإلكتروني للهجوم كساحة جديدة للصراع، معتبرةً إياه "نموذجاً استراتيجياً" للحروب المستقبلية، و حللت الأدوات التقنية المستخدمة في هجمات حجب الخدمة (DDoS) وآثارها على البنية التحتية الحيوية لإستونيا.

المنهجية: دراسة تحليلية وصفيّة.

خلصت إلى أن الهجوم كشف عن "فجوة خطيرة" في الموازنة الاستراتيجية بين الدول، حيث يمكن لدولة صغيرة أن تتعرض لتهديد وجودي من خلال أدوات غير مكلفة.

كما شددت على ضرورة أن تدرك الدول النامية أهمية تأمين فضاءها الإلكتروني كجزء من أمنها القومي، وأن تستثمر في بناء كفاءات وطنية في هذا المجال.

2- دراسة (**Tikk et al, 2010**) بعنوان: "الدفاع السيبراني في إستونيا: دروس من الهجمات الإلكترونية عام 2007"، هدفت إلى إعادة تعريف مفهوم "الهجوم" في عصر المعلومات، وحللت الإشكاليات القانونية الدولية، مثل صعوبة تطبيق مادة الدفاع الجماعي (المادة 5) في حالات الهجمات الإلكترونية ذات المصدر غير المؤكد.

المنهجية: تحليل قانوني وسياسي معمق من قبل باحثين في مركز التميز الذي أنشئ نتيجة مباشرة للهجوم.

خلصت إلى ضرورة التعاون بين القطاعين العام والخاص، وأهمية وجود سلطة وطنية موحدة لإدارة الأزمات السيبرانية.

كما أوصت بتطوير أطر قانونية دولية جديدة وأطر للثقة بين الدول لمواجهة هكذا تهديدات.

3- دراسة (**Ottis, 2010**) بعنوان: "المرونة السيبرانية: كيف حولت إستونيا الأزمة إلى فرصة"، هدفت إلى تسليط الضوء على الدور غير المسبوق للمجتمع المدني والتكنولوجي ("المتطوعون الإلكترونيون") كقوة مضادة للحملة المعلوماتية والمعرفية المعادية، وعلى مفهوم "المرونة السيبرانية" (Cyber Resilience) كعامل حاسم في هزيمة الهجوم.

المنهجية: تحليل استراتيجي لاستجابة إستونيا من منظور نظرية "الحرب المعلوماتية".

خلصت إلى أن الاستجابة الناجحة تتطلب مزيجاً من: الاستعداد التقني، والمرونة المؤسسية، والتماسك الاجتماعي، والدعم الدولي. وأن نجاح إستونيا في تحويل نفسها من "ضحية" إلى "رائد عالمي" في الأمن السيبراني كان من خلال إنشاء مركز التميز التابع للناتو (CCDCOE) وتعزيز التعاون الدولي.

4- دراسة (**Carmichael, 5, 2025**) بعنوان: "دروس من إستونيا الصغيرة والرقمية للغاية: صنع القرار في أعقاب أزمات الأمن السيبراني".

هدفت هذه الدراسة إلى تحليل عملية صنع القرار في إستونيا بعد أربع أزمات سيبرانية رئيسية: هجمات 2007، أزمة البطاقات الإلكترونية 2017، جائحة كوفيد-19، والحرب في أوكرانيا. كما سعت إلى استخلاص الدروس التي يمكن للدول الأخرى الاستفادة منها في إدارة الأزمات السيبرانية.

المنهجية: دراسة تحليلية مقارنة لأربع حالات من الأزمات السيبرانية، بالاعتماد على الوثائق الرسمية والمقابلات مع صناع القرار في إستونيا.

خلصت إلى أن نجاح إستونيا في تجاوز هذه الأزمات لم يكن وليد الصدفة، بل نتاج ثلاثة عوامل مترابطة: أولاً، وجود استراتيجية وطنية واضحة للأمن السيبراني تُحدد الأدوار والمسؤوليات. ثانياً، بناء الثقة بين القطاعين العام والخاص، وهو ما تجلى في التعاون الوثيق بين الحكومة وشركات التكنولوجيا والبنوك. ثالثاً، الاستثمار المستمر في رأس المال البشري والوعي المجتمعي.

5- دراسة (**Mölder, Sazonov & Loik, 2025**) بعنوان: "تحديات الأمن الداخلي في مواجهة التهديدات الهجينة الكامنة خلال الحرب في أوكرانيا: حالة إستونيا".

هدفت هذه الدراسة إلى تحليل طبيعة التهديدات الهجينة الكامنة (Latent Hybrid Threats) التي واجهتها إستونيا خلال الحرب الروسية على أوكرانيا (2022-2025)، وتقييم مدى جاهزية منظومة الأمن الداخلي الإستوني لمواجهتها. كما سعت إلى تقديم إطار مفاهيمي جديد لتصنيف هذه التهديدات التي تعمل تحت عتبة الحرب المفتوحة.

المنهجية: منهج دراسة الحالة، بالاعتماد على تحليل التقارير الرسمية الصادرة عن الحكومة الإستونية وحلف الناتو، بالإضافة إلى مصادر استخباراتية مفتوحة المصدر (OSINT).

خلصت إلى: أن التهديدات الهجينة الكامنة قد تطورت بشكل كبير بعد الغزو الروسي لأوكرانيا، حيث لم تعد تقتصر على الهجمات الإلكترونية والحملات المعلوماتية، بل امتدت لتشمل عمليات التأثير على الناخبين، واستغلال الضعفاء والمهمشين، والتجسس الصناعي، والهجمات على البنية التحتية الحيوية (مثل كابلات الطاقة والاتصالات البحرية). كما أوصت الدراسة بضرورة تعزيز التعاون بين أجهزة الاستخبارات المدنية والعسكرية، وتطوير آليات للكشف المبكر عن هذه التهديدات قبل تحولها إلى أزمات مكتملة.

6- دراسة (**Schultz, Smaliukiene & Giedraityte, 2025**) بعنوان: "المرونة الديمقراطية في دول البلطيق، المجلد الأول: الحوكمة المرنة والاستقرار الديمقراطي".

هدفت هذه الدراسة إلى تقديم إطار نظري وتحليلي لمفهوم "المرونة الوطنية" كما طبقته دول البلطيق (إستونيا، لاتفيا، ليتوانيا) في مواجهة التهديدات الهجينة. كما سعت إلى استخلاص آليات محددة طورتها هذه الدول للحفاظ على الاستقرار الديمقراطي وتعزيز المناعة المجتمعية في وجه حملات التضليل والتدخل الأجنبي.

المنهجية: منهج متعدد التخصصات يجمع بين التحليل السياسي والقانوني والاجتماعي، بالاعتماد على دراسة مقارنة لدول البلطيق الثلاث.

خلصت إلى: أن المرونة الوطنية ليست مجرد قدرة تقنية على صد الهجمات، بل هي منظومة متكاملة تشمل أربعة أبعاد رئيسية: البعد المؤسسي (فعالية المؤسسات الحكومية واستقلال القضاء)، والبعد المجتمعي (التماسك الاجتماعي والثقة بين أفراد المجتمع ومؤسساته)، والبعد الإعلامي (مستوى محو الأمية الإعلامية والمناعة ضد المعلومات المضللة)، والبعد الدولي (قوة التحالفات والتكامل مع هياكل الأمن الجماعي).

ما يميز هذا البحث عن الدراسات السابقة:

يمكن تقسيم الدراسات السابقة إلى مرحلتين: مرحلة مبكرة ركزت على تحليل هجمات 2007 مباشرةً، ومرحلة لاحقة تناولت تطور الحرب الهجينة وتطبيقاتها الأوسع.

أولاً: الدراسات المبكرة (2010) : ركزت كل منها على زاوية محددة. فدراسة العاني ركزت على البُعد التقني والإلكتروني معتبرةً الهجوم "نموذجاً للحرب الإلكترونية"، بينما حللت دراسة Tikk et al البُعد القانوني الدولي واستجابة الناتو، في حين تناولت دراسة Ottis استجابة إستونيا من منظور "المرونة السيبرانية".

ثانياً: الدراسات اللاحقة (2022–2025) : جاءت لتوسيع نطاق التحليل. فدراسة (**Carmichael, 2025**)حللت عملية صنع القرار الإستوني بعد أربع أزمات سيبرانية متعاقبة، ودراسة (**Mölder, Sazonov & Loik, 2025**) تناولت التهديدات الهجينة الكامنة خلال الحرب في أوكرانيا، في حين قدمت دراسة (**Schultz, Smaliukiene & Giedraityte, 2025**) إطاراً نظرياً شاملاً لمفهوم "المرونة الوطنية" في دول البلطيق.

أما هذا البحث فيتميز عن جميع ما سبق بالآتي: أولاً، يتبنى رؤية شمولية متكاملة تحت مظلة مفهوم "الحرب الهجينة"، لا يكتفي بتحليل بُعد واحد (كالإلكتروني أو القانوني)، بل يدمج جميع الأبعاد معاً (الإلكتروني، المعلوماتي، المدني، الاقتصادي، الدبلوماسي) ويُظهر كيف تفاعلت هذه الأبعاد بشكل متزامن. ثانياً، يتجاوز البحث نطاق الدراسات السابقة من خلال تتبع تطور الحرب الهجينة على إستونيا حتى عام 2025، ما يتيح استخلاص دروس محدثة حول بناء المرونة الوطنية في مواجهة التهديدات المتطورة.

إشكالية البحث:

تكمن الإشكالية الرئيسية لهذا البحث في السعي لتحليل أول حرب هجينة كبرى في العصر الرقمي من منظور استراتيجي شمولي. فعلى الرغم من صغر حجم إستونيا، إلا أنها قدمت نموذجاً معقداً للصراع الحديث الذي يتحدى المفاهيم التقليدية للحرب والسيادة. لذلك، تتحول إشكالية البحث من مجرد سرد الأحداث إلى السؤال الجوهري: كيف يمكن للدول، ولا سيما الصغيرة منها والمتوسطة، بناء منظومة مرونة وطنية متكاملة قادرة على الصمود في وجه الهجمات الهجينة التي تستهدف بشكل متزامن البنية التحتية الرقمية والنسيج الاجتماعي والاستقرار السياسي؟ وما هي الآليات الاستباقية والردية التي أثبتت فعاليتها في تحييد هذه التهديدات وتحويل الأزمة إلى فرصة لتعزيز الأمن القومي؟

أهمية البحث:

تتحدد أهمية هذا البحث في المستويين النظري والتطبيقي على النحو الآتي:

1. الأهمية الأكاديمية والنظرية:

تتمثل بسد فجوة معرفية في الأدبيات العربية من خلال تقديم دراسة تحليلية شاملة للحرب الهجينة، لا تقتصر على البعد التقني أو الإعلامي فحسب، بل تدمج جميع الأبعاد في إطار تحليلي موحد. وتطوير الإطار المفاهيمي للحرب الهجينة

والمرونة السيبرانية من خلال اختبارهما في حالة عملية، ما يثري النقاش الاستراتيجي حول طبيعة الصراع في القرن الحادي والعشرين.

2. الأهمية التطبيقية والاستراتيجية:

حيث يقدم البحث إطاراً عملياً لصانعي القرار في الدول النامية، يمكن الاستفادة منه في مراجعة استراتيجياتهم الأمنية، وخاصةً في مجالات الأمن السيبراني والأمن المعلوماتي. وتعزيز المرونة الوطنية، مثل شراكات القطاعين العام والخاص، وتمكين المجتمع المدني، وتعزيز المناعة المجتمعية ضد الحرب المعلوماتية، ما يوفر خارطة طريق للدول لتعزيز مناعتها الداخلية.

3. الاستفادة من الدروس الدولية:

تحويل الدروس المستفادة من تجربة إستونيا إلى توصيات قابلة للتطبيق في سياقات الدول النامية، مع الأخذ في الاعتبار الخصوصيات المحلية.

أهداف البحث:

1- تحليل طبيعة وأبعاد الهجوم الهجين على إستونيا عام 2007.

2- تقييم استجابة إستونيا لهذا الهجوم.

3- استخلاص الدروس الاستراتيجية والتشغيلية في مجالات الدفاع السيبراني، والتوعية المجتمعية، والتعاون الدولي.

4- تقديم توصيات قابلة للتطبيق للدول النامية.

فرضيات البحث:

الفرضية الرئيسية: كلما كانت منظومة المرونة الوطنية للدولة متكاملة ومتعددة المستويات (استراتيجية، تكتيكية، مجتمعية، دولية)، كلما زادت قدرتها على تحييد آثار الحرب الهجينة وتحويل التهديد إلى فرصة لتعزيز أمنها القومي.

ويتفرع عنها **الفرضيات الفرعية** الآتية:

1- يرتبط نجاح مواجهة الهجمات الإلكترونية بشكل مباشر بفعالية آليات التنسيق بين القطاعين العام والخاص ووجود سلطة سيبرانية موحدة.

2- يلعب مستوى الوعي المجتمعي والمناعة الإعلامية لدى المواطنين دوراً حاسماً في إفشال الحملات المعلوماتية المعادية، وهو ما لا يقل أهمية عن المواجهة التقنية.

3- يساهم الانتماء إلى تحالفات دولية فاعلة في رفع تكلفة الهجوم على الخصم ويعزز قدرات الردع والاستجابة للدول الصغيرة.

منهجية البحث:

تحقيقاً لأهداف البحث وحتى يمكن الإجابة عن تساؤلاته واختبار صحة الفرضيات، فقد تم استخدام منهج دراسة الحالة (Case Study Methodology)، مع الاستعانة بتحليل المحتوى للمصادر الأولية (تقارير حكومية، تصريحات مسؤولين) والثانوية (أبحاث، كتب، مقالات).

المطلب الأول: الإطار النظري والمفاهيمي للحرب الهجينة

لا يمكن فهم الحرب الهجينة بمعزل عن التطور التاريخي لنظريات الحروب، فهي ليست ظاهرة طارئة، بل نتاج طبيعي لتراكم الخبرات العسكرية والاستراتيجية عبر القرون. لهذا السبب، يستعرض هذا المطلب تطور أجيال الحروب الأربعة، من حروب الجيل الأول القائمة على الصفوف المتراصة إلى حروب الجيل الرابع القائمة على التمرد والحرب غير المتماثلة. ثم ينتقل إلى تعريف الحرب الهجينة كمفهوم متكامل، مستعرضاً أبرز تعريفاتها النظرية، ومحللاً أشكالها المتعددة (العسكرية، الإلكترونية، المعلوماتية، الدبلوماسية)، وخصائصها التي تجعل منها تحدياً فريداً للدول المعاصرة. هذا التأسيس النظري ضروري لفهم كيفية تطبيق هذه المفاهيم على حالة إستونيا في المطلب التالي.

أولاً: مفهوم الحرب الهجينة ونشأتها

لم يظهر مفهوم الحرب الهجينة (Hybrid Warfare) من فراغ، بل هو نتاج طبيعي لتطور نظريات الحروب عبر الأجيال، حيث يمكن تتبع هذا التطور بإيجاز على النحو الآتي[1]:

1- حروب الجيل الأول (1648-1860):

اعتمدت هذه الحروب على حشد أعداد كبيرة من القوات في صفوف متراصة لتوجيه نيران كثيفة ومتزامنة نحو العدو، وكان الهدف الأساسي هو تحقيق انتصار عسكري حاسم من أول مواجهة، كما في الحروب النابليونية (1803-1815). ورغم أن هذا الجيل من الحروب ساهم في غرس ثقافة النظام والانضباط العسكري التي لا تزال تمثل سمة رئيسية في الجيوش الحديثة، إلا أن تطور الأسلحة الآلية لاحقاً جعل تكتيكات "الصفوف" عقيمة وانتحارية، ما استدعى الانتقال إلى أنماط قتالية جديدة.

2- حروب الجيل الثاني (1860-1918):

مع التطور التكنولوجي وانتشار البنادق الآلية والمدرعات الثقيلة، تراجعت تكتيكات الصفوف لصالح الاعتماد على الخنادق، وتحول الهدف من النصر الحاسم إلى استنزاف العدو وإرهاقه. فقد قامت هذه الحروب على التنسيق بين أسلحة المدفعية والمشاة والمدرعات، مع التركيز على الطاعة والمنهجية والاعتقاد بوجود حلول نظامية لكل المشكلات. كما تُعد الحرب العالمية الأولى (1914-1918) المثال الأبرز لهذا الجيل، الذي ارتبط بظهور الطائرات المقاتلة والاعتماد على الاقتصاد الصناعي للإنتاج العسكري بكميات ضخمة.

3- حروب الجيل الثالث (1918-1990):

ظهرت مع الحرب العالمية الثانية (1939-1945) عندما طبق الألمان نمط "الحروب الخاطفة"، القائم على المناورة السريعة بدلاً من الاستنزاف البطيء، من خلال الالتفاف على قوات العدو وقطع خطوط إمداداته وتدمير مراكز القيادة والسيطرة. وقد ساعد في ظهور هذا الجيل تطور الدبابات والطائرات ونظم الاتصالات، ما سمح بالتنسيق بين القوات البرية والجوية بدرجة غير مسبوقة. حيث تراجعت ثقافة الانضباط الصارم لصالح المبادرة واللامركزية في اتخاذ القرار، ما مكن جيشاً أقل عدداً من هزيمة جيش أكبر، كما حدث في معركة فرنسا (1940).

4- حروب الجيل الرابع:

تعتمد حروب هذا الجيل على توظيف أسلوب حركات التمرد، وقد حدد "ماو تسي تونج" ثلاث مراحل لنجاحها: الأولى بناء الدعم السياسي عبر الاغتيالات والحملات الدعائية، والثانية السيطرة على مناطق متنازع عليها وحكمها، والثالثة التحول إلى جيش نظامي لإسقاط الحكومة. أما الهدف الاستراتيجي لها فهو إقناع صانع القرار لدى الخصم بأن أهدافه إما غير قابلة للتحقيق أو أنها مكلفة للغاية مقارنة بالعوائد المتوقعة.

وتندرج الحرب الهجينة ضمن سياق تطور هذا الجيل وصولاً للجيل الخامس من الحروب، بل يمكن اعتبارها تجسيداً عملياً متطوراً له، حيث تمزج بين الأدوات التقليدية (كالقوة العسكرية المحدودة) وغير التقليدية (كالهجمات الإلكترونية والحملات المعلوماتية) بشكل متزامن ومتعاضد.

فقد عرَف فرانك هوفمان – وهو من أبرز المنظرين للمفهوم– الحرب الهجينة بأنها "مزيج متزامن ومترابط من الوسائل التقليدية وغير التقليدية، النظامية وغير النظامية، بما في ذلك الحملات التخريبية والإجرامية وأعمال العنف، بهدف تحقيق مكاسب سياسية". يتميز هذا النوع من الحروب بأنه يطمس الخطوط الفاصلة بين حالة الحرب والسلم، وبين المقاتل والمدني، وبين الجبهة الداخلية والخارجية.[2]

حيث تستفيد الحرب الهجينة من تعقيدات العولمة والتقدم التكنولوجي، وخاصةً في مجالات الاتصال والمعلومات. فهي لا تسعى بالضرورة إلى تحقيق انتصار عسكري ساحق، بل إلى إرباك الخصم، وتآكل قدرته، وتقويض شرعيته، وزعزعة استقراره الداخلي، وبالتالي إجباره على قبول شروط المهاجم السياسية بثمن بخس نسبياً.

ثانياً: أشكال الحرب الهجينة

يمكن تقسيم أشكال الحرب الهجينة إلى عدة مكونات رئيسية تتفاعل فيما بينها بشكل متزامن ومتعاضد، منها:

1– المكون العسكري التقليدي المحدود: لا يتم التخلي كلياً عن القوة العسكرية، لكنها تستخدم بشكل محدود ومحسوب، وغالباً ما تكون مقنعة أو منكرة. قد يتجلى ذلك في مناورات عسكرية على الحدود، أو اختراقات جوية وبحرية متعمدة، أو استخدام قوات خاصة أو مرتزقة. الهدف هو التهديد والردع دون الدخول في حرب شاملة.[3]

2– المكون الإلكتروني (السيبراني): يعد الفضاء الإلكتروني ساحة رئيسية في الحرب الهجينة. حيث تشمل الهجمات الإلكترونية عمليات حجب الخدمة الموزع (DDoS)، والاختراق والتجسس، وتعطيل البنية التحتية الحيوية (كشبكات الكهرباء والاتصالات والمرافق المالية)، وتخريب البيانات. يتميز هذا المكون بتكلفته المنخفضة نسبياً، وصعوبة نسب المصدر، وتأثيره المدمر على اقتصاد الدولة وخدماتها.[4]

3– المكون المعلوماتي والإعلامي: تمثل الحرب المعلوماتية (Information Warfare) القلب النابض للحرب الهجينة. تهدف إلى "كسب القلوب والعقول" من خلال استخدام الدعاية، والشائعات، والأخبار المزيفة، والتضليل الإعلامي، بهدف تشويه صورة الخصم، وتبرير أفعال المهاجم، وتعميق الانقسامات الداخلية في المجتمع المستهدف، وزعزعة ثقة المواطنين بحكومتهم. كما تستغل هذه الحملات وسائل الإعلام التقليدية ومواقع التواصل الاجتماعي على حد سواء.[5]

4– استخدام الوكلاء والجماعات غير التابعة للدولة: لتوفير "الإنكار المعقول" (Plausible Deniability)، يعمد المهاجم إلى استخدام وكلاء محليين أو جماعات متمردة أو عصابات إجرامية لتنفيذ بعض العمليات، مثل إثارة الاضطرابات المدنية أو تنفيذ هجمات إرهابية. هذا يجعل من الصعب إثبات تورط الدولة مباشرةً.[6]

5– الضغوط الاقتصادية والسياسية: يتم استخدام أدوات القوة الناعمة والذكية لممارسة الضغط، مثل فرض حظر اقتصادي غير معلن، وعمليات المقاطعة، واستخدام الطاقة كسلاح، وممارسة الضغوط الدبلوماسية في المحافل الدولية لعزل الدولة المستهدفة.

ثالثاً: خصائص الحرب الهجينة

يمكن إيجاز أهم خصائص الحروب الهجينة على النحو الآتي:

1– **الاعتماد على الهجمات السيبرانية:**

تتسم الحروب الهجينة بالاعتماد المتزايد على القوة السيبرانية. حيث يتم تنفيذ الهجمات السيبرانية على البنية التحتية الحيوية للعدو، مثل الأنظمة العسكرية، والشبكات الكهربائية، ووسائل الإعلام. كما يتم استخدام أساليب الحرب الإلكترونية للتشويش على الاتصالات وتعطيل عمليات العدو، ما يؤثر على فعالية الاستجابة العسكرية. هذه الجوانب تشكل جزءاً حيوياً من استراتيجية الحرب الحديثة.[7]

2-زيادة التعقيد العسكري:

تمكنت الفواعل المسلحة من دون الدول في توظيف منظومات أسلحة متطورة، ومن ذلك أنظمة الصواريخ المضادة للسفن، والدرونز الجوية، بالإضافة إلى قدرتها على استخدام النظم التكنولوجية المتقدمة مثل الاتصالات السيبرانية المؤمنة، ونظم القيادة والسيطرة المعقدة، بالإضافة إلى بعض التكتيكات التي كانت محصورة بالجيوش، مثل "الجمع بين الأسلحة" و الذي يهدف إلى توظيف أكثر من سلاح، مثل الجمع ما بين المشاة والمدرعات، بشكل متزامن من أجل تكبيد الخصم خسائر عسكرية كبيرة. ولا يجب إغفال أن الفواعل المسلحة من دون الدول بات بإمكانها امتلاك القدرات السيبرانية، وتوظيفها بشكل متزايد في مواجهة الدول المتقدمة وقواتها المسلحة. ولعل هذا ما يميز الحروب الهجينة في القرن الحادي والعشرين عن القرن العشرين، حيث أصبح البعد الجديد هو تمكن هذه الفواعل من الحصول على أنظمة قتالية وتكنولوجية وسيبرانية متقدمة كانت تقتصر على الجيوش وحدها. كما في [1]

3-تزايد الاعتماد على الوسائل غير العسكرية أو التوسع الأفقي:

تتميز الحروب الهجينة بالتنوع في الوسائل المستخدمة. حيث تتجلى هذه الظاهرة في انفتاح الحروب على مختلف الأدوات والموارد، من القوى المسلحة النظامية إلى التقنيات الحديثة مثل الطائرات الأوتوماتيكية دون طيار والروبوتات العسكرية. وهذا يُمكّن الأطراف الفاعلة من تكييف استراتيجياتهم بشكل مرن استجابةً لتغيرات الميدان، حيث يعتمد الفاعلون في الحروب الهجينة على أساليب متنوعة لتحقيق أهدافهم في مواجهة تعقيدات الصراع.[8]

4-التدخل العسكري المباشر:

رغم أن الحروب الهجينة لا يتم الإعلان عنها، وقد تندلع فجأة وبدون سابق إنذار، كما أنه لا يمكن التنبؤ بمساراتها، فإنه يمكن توظيف التدخل العسكري المباشر من قبل إحدى الدول، تحت ادعاء القيام بعمليات حفظ السلام.

وإذا كانت الحرب تبدأ من خلال قيام أحد الأطراف المتصارعة بإثارة الاضطرابات، وتوظيف الدعاية الإعلامية المكثفة من أجل محاولة الحصول على دعم شعبي ودولي، وتصوير المحاولات الحكومية لاستعادة الاستقرار باعتبارها إحدى أدوات القمع، فإن عدم نجاح هذه العمليات في إضعاف الدولة، يدفع الدول الداعمة لها إلى التدخل العسكري المباشر، سواءً من خلال إرسال القوات الخاصة، أو من خلال الحصول على تصريح من الأمم المتحدة بهدف تحجيم قدرة الدولة في استعادة السيطرة على أراضيها.[9]

ويمكن إضافة عدد من الخصائص التي تجعل مواجه الحرب الهجينة صعبة ومعقدة:[10]

1-الإنكار المعقول (Plausible Deniability): تصمم العمليات بحيث يصعب إثبات تورط دولة ما بشكل قاطع، ما يعيق عملية الرد أو الردع.

2- الغموض وعدم الوضوح (Ambiguity): يصعب تحديد متى تبدأ الحرب ومتى تنتهي، وما إذا كانت حرباً أم مجرد أعمال استفزازية.

3-استهداف نقاط الضعف: تركز على استغلال الثغرات في المجتمعات الديمقراطية المفتوحة، كحرية الإعلام والشفافية والانقسامات السياسية والاجتماعية.

4-استغلال الفجوات القانونية: تستغل الغموض في القوانين الدولية فيما يخص الفضاء الإلكتروني والحرب المعلوماتية.

5-التكلفة المنخفضة والعائد المرتفع: توفر هذه الأساليب تأثيراً استراتيجياً كبيراً مقارنة بالتكاليف المالية والبشرية المحدودة.

يُظهر التحليل النظري أن الحرب الهجينة تمثل تحدياً وجودياً للدول، خاصةً الصغيرة منها، لأنها تستهدف بشكل متعمد نقاط ضعفها الاستراتيجية في الفضاءات الرقمية والمجتمعية. غموض هذه الحروب وإنكار المسؤولية يعطلان آليات الردع التقليدية، ما يفرض تطوير مفاهيم أمنية جديدة. وبالتالي فإن الفهم العميق لهذا المفهوم هو الخطوة الأولى لبناء دفاعات فعالة، حيث أن الاعتراف بالتهديد شرط أساسي لمواجهته.

المطلب الثاني: دراسة حالة: الهجوم الهجين على إستونيا (2007)

بعد وضع الإطار النظري للحرب الهجينة، ينتقل هذا المطلب إلى تحليل حالة إستونيا كنموذج تطبيقي حي. ففي نيسان 2007، تعرضت هذه الدولة الصغيرة لهجمة متعددة الأبعاد شكلت أول حرب هجينة واسعة النطاق في العصر الرقمي. يبدأ المطلب باستعراض السياق التاريخي والسياسي الذي مهّد لهذا الهجوم، مع التركيز على التراكمات الجيوسياسية بين روسيا والغرب، ومعركة الذاكرة التاريخية حول التراث السوفيتي. ثم يحلل المطلب الأبعاد الأربعة للهجوم (الإلكتروني، المعلوماتي، المدني، الدبلوماسي) باستخدام جداول كمية توضح حجم الأضرار والآثار. وأخيراً، يقيم استجابة إستونيا السريعة على المستويات التقنية والمجتمعية والدولية، مبرزاً العوامل التي ساعدتها على الصمود وتحويل الأزمة إلى فرصة.

أولاً: السياق التاريخي والسياسي

لم يكن الهجوم على إستونيا عام 2007 مجرد رد فعل لحظي على نقل تمثال "الجندي البرونزي"، بل جاء نتيجة تراكمات جيوسياسية عميقة تعكس تحولات النظام العالمي بعد الحرب الباردة. فمع انهيار الاتحاد السوفيتي عام 1991، بدأت موسكو تفقد تدريجياً نفوذها التقليدي في أوروبا الشرقية، في مقابل تمدد غربي غير مسبوق تمثل بثلاث موجات متتالية من توسع حلف الناتو أعوام 1999 و2004 و2009. وقد كانت إستونيا، إلى جانب جاراتها من دول البلطيق، من بين الدول التي انضمت إلى الحلف عام 2004، وهو ما مثل – من منظور المدرسة الواقعية في العلاقات الدولية – تحدياً استراتيجياً مباشراً للأمن القومي الروسي، حيث تقلصت المنطقة العازلة التي طالما اعتبرتها موسكو ضرورية لسلامتها.[11]

وإذا كان التمدد الغربي يمثل البعد الجيوسياسي للصراع، فإن "معركة الذاكرة التاريخية" (Memory Wars) تمثل بعده الثقافي والمعرفي. فبينما تصر دول البلطيق على وصف الفترة الممتدة من 1940 إلى 1991 بأنها سنوات احتلال سوفيتي قاسٍ، تروّج موسكو لرواية مغايرة تصفها بأنها "تحرير من النازية" واندماج طوعي. وعلى هذا الأساس، تحولت الرموز التاريخية – كالنصب التذكارية وأسماء الشوارع – إلى ساحات حرب بالوكالة، يتجدد الصراع عليها كلما حاولت إحدى الدول إعادة كتابة تاريخها بما يتوافق مع هويتها الوطنية. كما في[6]

في هذا السياق المتوتر، شكلت إستونيا – بحكم موقعها كدولة حدودية (Borderland) بين الغرب وروسيا، وصغر حجمها النسبي، واعتمادها الاستثنائي على التحول الرقمي (حكومة إلكترونية، مجتمع رقمي) – هدفاً مثالياً لاختبار فعالية استراتيجيات الحرب الهجينة. فالنجاح في مهاجمة إستونيا، حتى دون إعلان حرب رسمي، كان سيرسل رسالة

ردع واضحة إلى دول البلطيق وبولندا ودول الكتلة الشرقية السابقة مفادها: أن الاندماج الغربي له ثمن باهظ، وأن روسيا لا تزال تمتلك أدوات ناعمة وصلبة قادرة على فرض نفوذها ومنع المزيد من التمدد الغربي في محيطها الحيوي. كما في [10]

فقد كانت الشرارة المباشرة للهجوم هي قرار الحكومة الإستونية برئاسة أندروس أنسيب بنقل نصب "الجندي البرونزي" التذكاري – وهو نصب تذكاري للجنود السوفيت– من وسط العاصمة تالين إلى مقبرة عسكرية في ضواحيها في 26 نيسان 2007. من المنظور الإستوني، كان هذا التمثال يمثل رمزاً لخمسين عاماً من الاحتلال السوفيتي القاسي. أما من المنظور الروسي والمجتمع الناطق بالروسية داخل إستونيا (الذي يشكل حوالي 25% من السكان)، فقد كان يمثل تحريراً من النازية وتذكاراً لشهداء الحرب العالمية الثانية. حيث عبر رئيس الوزراء أنسيب عن موقف حكومته بالقول: "لا يمكن أن يظل رمز للاحتلال والاستبداد في وسط عاصمة دولة أوروبية حرة".[12]

ثانياً: تحليل الهجوم: مزيج متعدد الأبعاد

كان الهجوم على إستونيا نموذجاً مثالياً للحرب الهجينة، حيث ضرب بأبعاده الأربعة بشكل متزامن ومتعاضد.

1- الهجوم الإلكتروني:

بدأت سلسلة من هجمات حجب الخدمة الموزعة (DDoS) غير المسبوقة في 27 نيسان واستمرت على موجات متقطعة لمدة ثلاثة أسابيع. كما وصف تقرير مركز الاستجابة للطوارئ الحاسوبية الإستوني (CERT-EE) الهجمات بأنها "مستوى جديد من التهديد"، مستهدفةً "البنية التحتية الحيوية للإنترنت في البلاد". حيث شملت الهجمات:[13]

- القطاع المالي: تعطيل خدمات الإنترنت للبنوك الكبرى مثل هانسابانك وسي إي بي، ما منع المواطنين من الوصول إلى حساباتهم.
- القطاع الحكومي: إسقاط مواقع البرلمان والوزارات والشرطة، ما عطل الخدمات الإلكترونية.
- وسائل الإعلام: تعطيل مواقع الصحف والإذاعات الرئيسية، ما أعاق تدفق المعلومات الموثوقة.

كما أشار التقرير إلى تعقيد الهجمات واستخدامها لأساليب مثل "تسمم DNS" وشبكات البوت نت الضخمة، ما يشير إلى تنسيق عال المستوى. والجدول الآتي يوضح حجم الهجوم الالكتروني على إستونيا:

الجدول رقم (1): تحليل الهجمات الإلكترونية على إستونيا (نيسان-أيار 2007)

القطاع المستهدف	عدد المواقع المتأثرة	نوع الهجوم	مدة التعطيل	التكلفة التقديرية
القطاع الحكومي	15 موقعاً	اختراق DDoS	3-7 أيام	100 مليون كرون
القطاع المالي	12 موقعاً	مكثف DDoS	2-5 أيام	250 مليون كرون
وسائل الإعلام	23 موقعاً	تشويه DDoS	1-3 أيام	50 مليون كرون
البنية التحتية للاتصالات	8 أنظمة	تعطيل DDoS	4-6 أيام	150 مليون كرون

المصدر: من إعداد الباحث اعتماداً على [13]

يكشف الجدول رقم (1) عن الطابع المنهجي والمنظم للهجوم الإلكتروني، حيث استهدف بشكل متعاقب ومتزامن القطاعات الحيوية للدولة الإستونية. تشير دقة استهداف البنية التحتية الرقمية للحكومة والقطاع المالي – وهي شريان حياة الدولة الحديثة – إلى وجود دراسة مسبقة معمقة لنقاط الضعف الإستونية. كما أن تزامن ذروة الهجمات مع الأحداث السياسية على الأرض يؤكد الطابع التكتيكي المنسق لهذا البعد من الحرب الهجينة، ويدحض رواية كونه هجوماً عشوائياً من قراصنة مستقلين.

2- الهجوم المعلوماتي:

عملت حملة معلوماتية مكثفة بالتوازي مع الهجمات الإلكترونية. حيث قامت وسائل الإعلام الروسية والقنوات الناطقة بالروسية داخل إستونيا بحملة تحريضية، وروجت لروايات مفادها أن الحكومة الإستونية "تدنس ذكرى الشهداء" و"تمجد النازية". كما أشار تقرير للجنة الأوروبية لمكافحة العنصرية وكراهية الأجانب (ECRI) إلى أن "التغطية الإعلامية باللغة الروسية كانت تحريضية بشكل كبير وساهمت في تأجيج المشاعر". أما الهدف فهو: زعزعة الاستقرار الداخلي من خلال تعميق الانقسام الإثني بين الإستونيين والناطقين بالروسية، وتشويه صورة إستونيا دولياً.[14] والجدول الآتي يوضح حجم الهجوم المعلوماتي على إستونيا:

الجدول رقم (2): تحليل الحملة المعلوماتية ضد إستونيا

الوسيلة الإعلامية	نوع المحتوى	اللغة	الجمهور المستهدف	التكرار اليومي
القنوات الروسية الرئيسية	تقارير تحريضية	الروسية	الناطقون بالروسية	10–15 تقريراً
مواقع الإنترنت	أخبار مزيفة، شائعات	الروسية، الإستونية	المجتمع الدولي	50–100 مقال يومي
الإذاعات المحلية	خطابات تحريضية	الروسية	سكان تالين	20–30 بثاً يومياً
منصات التواصل	منشورات مضللة	متعددة	الشباب الإستوني	1000 منشور

المصدر: من إعداد الباحث اعتماداً على [14]

يوضح الجدول رقم (2) تنوع وانتظام الأدوات المستخدمة في الحملة المعلوماتية، حيث تم تصميم رسائل مختلفة بلغات متعددة لتستهدف شرائح مجتمعية محددة. يشير التكرار اليومي المرتفع للمحتوى الإعلامي – خاصةً على المنصات الرقمية – إلى وجود خطة إعلامية ممنهجة تهدف إلى تحقيق التغطية المستدامة والتأثير التراكمي. لقد مثلت هذه الحملة الذراع النفسي للحرب الهجينة، التي سعت إلى كسب المعركة في عقول المواطنين قبل ساحات القتال.

3- الاضطرابات المدنية:

تحولت الاحتجاجات على نقل التمثال إلى أعمال شغب وعنف في شوارع تالين لمدة ليلتين متتاليتين. قام متظاهرون، معظمهم من الشباب الناطقين بالروسية، بتكسير النوافذ وحرق السيارات ونهب المحال التجارية. وفقاً لتقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، أسفرت الاشتباكات مع الشرطة عن "مقتل مواطن روسي واحد وإصابة 156 شخصاً، بينهم 44 ضابط شرطة". شكلت هذه الاضطرابات الذراع "المادي" للهجوم الهجين، ما أجبر السلطات على تشتيت مواردها بين إدارة الأزمة الإلكترونية واستعادة النظام العام.[15] والجدول الآتي يوضح ذلك:

الجدول رقم (3): تحليل الاضطرابات المدنية في تالين (26–28 نيسان 2007)

المؤشر	العدد	التوزيع	النتائج المباشرة
عدد المتظاهرين	2000 تقريباً	مركزية في وسط تالين	أعمال شغب وتخريب
الإصابات	156 شخصاً	112 مدنياً، 44 شرطة	عنف واستخدام القوة
الاعتقالات	1000 قضية	100 اعتقال فوري	تحقيقات جنائية
الأضرار المادية	50 متجراً	تكسير وحرق	خسائر تجارية

المصدر: من إعداد الباحث اعتماداً على [15]

يظهر الجدول رقم (3) كيف تحولت الاحتجاجات السلمية إلى أعمال شغب منظمة، ما يؤشر إلى وجود تحريض مسبق وتخطيط لتحقيق أقصى قدر من التدمير والاضطراب. حيث يشير التركيز الجغرافي للاحتجاجات في العاصمة تالين – مركز القرار السياسي والإداري – إلى استهداف مقصود لرمزية الدولة ومركز قوتها. كما أن هذا البعد المادي من الهجوم الهجين هدف إلى إرباك أجهزة الأمن وإشغالها عن مواجهة الأبعاد الأخرى للهجوم.

4- الضغط الدبلوماسي والاقتصادي:

على المستوى الدبلوماسي، شنت روسيا هجوماً سياسياً على الحكومة الإستونية، واتهمتها بـ"الهمجية". على الأرض، فرضت حصاراً اقتصادياً غير معلن، حيث أوقفت شحنات النفط وعطلت حركة الشحن عبر الحدود البرية. حيث ذكر بيان لوزارة الخارجية الإستونية أن "حركة الشحن عبر الحدود البرية بين إستونيا وروسيا قد توقفت فعلياً. وكان الهدف من هذا الضغط المزدوج عزل إستونيا دولياً وإلحاق خسائر اقتصادية بها لإجبارها على التراجع.[16] والجدول الآتي يوضح ذلك:

الجدول رقم (4): أدوات الضغط الدبلوماسي والاقتصادي

نوع الضغط	لأدوات المستخدمة	المدة	التأثير
الضغط الدبلوماسي	احتجاجات رسمية، اتهامات علنية	3 أسابيع	عزل دبلوماسي
الحصار الاقتصادي	تعطيل شحنات النفط، إغلاق حدود	10 أيام	خسائر تجارية
المقاطعة	مقاطعة البضائع الإستونية	شهرين	تراجع الصادرات
الضغط السياسي	تهديدات غير مباشرة	مستمر	توتر سياسي

المصدر: من إعداد الباحث اعتماداً على [16]

يكشف الجدول رقم (4) عن الاستخدام الاستراتيجي لأدوات القوة الناعمة والذكية لممارسة الضغط على الدولة الإستونية من خلال قنوات متعددة. حيث يبرز الجدول كيف تم تصميم هذه الضغوط لتكون متدرجة ومستدامة، ما يخلق تأثيراً تراكمياً على قدرة الدولة على الصمود. إن تعدد الأدوات وتنوعها – من الدبلوماسية إلى الاقتصاد – يؤكد النهج الشامل للحرب الهجينة، الذي يسعى لإضعاف الدولة من خلال ضرب مصادر قوتها المختلفة.

ثالثاً: استجابة إستونيا: المرونة في مواجهة العاصفة

واجهت إستونيا، هذا الهجوم المتعدد الجوانب باستجابة متعددة المستويات أظهرت درجة عالية من المرونة والابتكار، نوضحها بالآتي:

1- الاستجابة التقنية والسيبرانية الفورية:

تحرك الفنيون والإداريون في إستونيا بسرعة لحماية البنية التحتية الرقمية. فقد قام مركز CERT-EE بتنسيق جهود تضمنت:

· عزل الخوادم المستهدفة: فصل الخوادم الحيوية عن الإنترنت العام مؤقتاً.

· تصفية حركة المرور: التعاون مع مقدمي خدمات الإنترنت (ISPs) لتصفية حركة المرور الضارة القادمة من خارج البلاد، مع تطبيق حظر جغرافي جزئي.

· توزيع الحمولة: نقل الخدمات الحيوية إلى خوادم احتياطية ومواقع استضافة في دول صديقة مثل فنلندا والسويد. كما في [13]

2- دور المجتمع المدني والتكنولوجي:

برز هنا عنصر فريد في القصة الإستونية، وهو دور "المجتمع الرقمي". فقد تجمع متطوعون من خبراء الأمن الإلكتروني والمواطنين العاديين في منتديات عبر الإنترنت (أبرزها موقع "أوبن نت") لتنسيق الجهود. ساعد هؤلاء "المتطوعون الإلكترونيون" في تحليل رزم البيانات، وتتبع مصادر الهجمات، وحماية المواقع الصغيرة. كما علقت مجلة الإيكونوميست على هذه الظاهرة بأنها "شكل من أشكال الدفاع المدني الرقمي، حيث قام المواطنون بحماية وطنهم من خلف شاشات حواسيبهم".[17]

3- اللجوء إلى حلف الناتو والمجتمع الدولي:

بعد أن فاقت الهجمات قدراتها الوطنية، التمست إستونيا الدعم من حلفائها. على الرغم من أن الهجوم لم يندرج تحت المادة الخامسة من ميثاق الناتو (التي تنص على أن الهجوم على عضو هو هجوم على الكل)، إلا أنه أثار نقاشاً حاداً داخل الحلف حول طبيعة التهديدات في القرن الحادي والعشرين. حيث أرسلت دول أعضاء في الناتو خبراء في مجال الأمن الإلكتروني لمساعدة إستونيا. وبالتالي كان الرد الدولي، وخاصةً من الناتو، إشارةً مهمةً مفادها: أن الهجمات الإلكترونية لن تمر دون رد.[18]

وأدى هذا الحدث مباشرةً إلى تسريع إنشاء مركز التميز للدفاع السيبراني التعاوني التابع للناتو (CCDCOE) في تالين عام 2008، ما حول إستونيا من ضحية إلى مركز عالمي للخبرة في الدفاع السيبراني.

تثبت حالة إستونيا أن الهجمة الهجينة تعمل كأوركسترا مدمرة، حيث يؤدي تزامن الهجمات الإلكترونية والمعلوماتية والمدنية إلى تضخيم الأثر. إن نجاح إستونيا النسبي لم يأت من مناعة مطلقة، بل من مرونة واستجابة سريعة ومتعددة المستويات. وبالتالي فإن الدرس الأساسي هنا هو أن وحدة الصف الوطني والتعاون بين الحكومة والمواطنين والقطاع الخاص يحولان الهشاشة الرقمية إلى قوة، وأن التحالفات الدولية تشكل شبكة أمان حيوية للدول الصغيرة. والجدول الآتي يوضح آليات الاستجابة الإستونية:

الجدول رقم (5): فعالية آليات الاستجابة الإستونية

آلية الاستجابة	الوقت المستغرق	عدد المشاركين	نسبة النجاح
عزل الخوادم الحيوية	2–6 ساعات	20 خبيراً	%90
تصفية حركة المرور	4–8 ساعات	50 فني اتصالات	%85
المتطوعون الإلكترونيون	12 ساعة	100 متطوع	%70
الدعم الدولي	24–48 ساعة	12 دولة	%95

المصدر: من إعداد الباحث اعتماداً على [19]

يوضح الجدول رقم (5) فعالية نموذج المرونة متعدد المستويات الذي تبنته إستونيا في مواجهة الأزمة. وتشير نسب النجاح المرتفعة – خاصةً في آليات الاستجابة التقنية والدولية – إلى أهمية التخطيط المسبق ووجود استراتيجية واضحة. كما يكشف الجدول عن الظاهرة الفريدة لـ "المتطوعين الإلكترونيين" كقوة رديفة رسمية، ما يؤكد دور المجتمع المدني كشريك استراتيجي في بناء المرونة الوطنية في مواجهة التهديدات الهجينة.

المطلب الثالث: تحليل النتائج واستخلاص الدروس المستفادة من تطور الحرب الهجينة على إستونيا (2007–2025)

بعد تحليل تفاصيل الهجوم والاستجابة الإستونية في المطلب الثاني، ينتقل هذا المطلب إلى المستوى التحليلي واستخلاص الدروس، مع توسيع الأفق الزمني ليشمل الفترة الممتدة من 2007 حتى 2025. حيث يبدأ المطلب بتقييم نتائج الهجوم المباشرة وغير المباشرة، موضحاً كيف فشلت استراتيجية المهاجم في تحقيق أهدافها بل حققت نتائج عكسية على المدى البعيد. ثم يتوسع المطلب ليتتبع تطور الحرب الهجينة على إستونيا خلال العقدين التاليين، مستعرضاً التهديدات الجديدة التي ظهرت بعد 2014 وكيف طورت إستونيا منظومتها الدفاعية لمواجهتها. وأخيراً، يستخلص المطلب الدروس المستفادة على المستويات الاستراتيجية والتشغيلية والدولية، مع التركيز على خمس دروس إضافية مستفادة من التطور الإستوني حتى عام 2025، والتي تقدم نموذجاً متكاملاً للمرونة الوطنية في العصر الرقمي.

أولاً: تحليل نتائج الهجوم

على الرغم من حدة الهجوم وتعدده، فإنه فشل في تحقيق هدفه الأساسي المتمثل في إسقاط الحكومة الإستونية أو إجبارها على التراجع عن سياستها الغربية. بل على العكس، يمكن القول إن الهجوم حقق نتائج عكسية على المدى المتوسط والطويل، من خلال:[20]

1-تعزيز الهوية الوطنية والتماسك الاجتماعي: على الرغم من محاولات تعميق الانقسام، فإن الهجوم عزز الشعور بالهوية الوطنية لدى غالبية الإستونيين، وأجبر النخب السياسية على التوحد في مواجهة التهديد الخارجي.

2-تسريع التحديث السيبراني: فقد أجبر الهجوم إستونيا على تسريع استثماراتها في مجال الأمن السيبراني، ما جعلها واحدة من أكثر الدول تقدماً في هذا المجال على مستوى العالم.

3-تعزيز مكانة إستونيا في الناتو: بدلاً من عزل إستونيا، عزز الهجوم مكانتها داخل حلف الناتو، حيث أصبحت "دولة رائدة" في مجال الدفاع السيبراني وأمن الفضاء الإلكتروني.

ثانياً: تطور الحرب الهجينة على إستونيا بعد 2007: من الدفاع إلى الريادة

لم تتوقف التهديدات الهجينة على إستونيا عند هجمات نيسان 2007، بل تطورت وتنوعت في العقدين التاليين لتشمل أدوات أكثر تعقيداً، وفي المقابل طورت إستونيا منظومة دفاعية متكاملة جعلتها واحدة من أكثر دول العالم مرونة في مواجهة هذه التهديدات. [21] ويمكن تتبع هذا التطور من خلال ثلاثة محاور رئيسية:

1- تطور التهديدات الهجينة (2014-2025)

مع تصاعد التوترات الجيوسياسية بعد ضم روسيا لشبه جزيرة القرم عام 2014، ثم الغزو الشامل لأوكرانيا عام 2022، تحولت التهديدات الهجينة ضد إستونيا من هجمات إلكترونية بشكل رئيسي إلى مزيج أكثر تنوعاً وتعقيداً. فقد شهدت إستونيا في هذه الفترة:[22]

· الحرب المعلوماتية والدعاية المستهدفة: تستهدف الدعاية الروسية بشكل خاص كبار السن الذين يحنون للعصر السوفيتي، وتصور إستونيا على أنها "دولة فاشلة"، كما تستغل الانقسامات المجتمعية القائمة وتزيد من استقطابها، خاصة مع اقتراب المواسم الانتخابية.

· الحوادث الحدودية والعسكرية: شهدت إستونيا في أيار 2024 قيام جنود روس بإزالة 25 من أصل 50 طافية حدودية كانت قد وضعتها إستونيا على نهر نارفا، وفي أيلول 2025 اخترقت طائرات حربية روسية من طراز MiG-31 الأجواء الإستونية لمدة 12 دقيقة.

· الهجمات على البنية التحتية الحيوية: في كانون الأول 2024، تم قطع كابل الطاقة البحري Estlink 2 الذي يربط إستونيا بفنلندا، على ما يعتقد أنها يد سفن تابعة لـ"الأسطول الظل" الروسي، كما شهدت مدينة نارفا انقطاعاً في التيار الكهربائي نتيجة عمل تخريبي محتمل.

· التضليل الإعلامي الرقمي: مع اقتراب الانتخابات المحلية عام 2025، برزت المعلومات المضللة كتهديد محسوب للديمقراطية الإستونية، حيث تستخدم الروبوتات (Bots) والشبكات المزيفة لنشر روايات متضاربة تهدف إلى زعزعة الثقة في العملية الانتخابية.

ويُلاحظ أن هذه التهديدات لم تعد تقتصر على البعد السيبراني فحسب، بل أصبحت هجينة بامتياز، تمزج بين الأدوات المادية (قطع الكابلات، انتهاك الأجواء، التخريب الحدودي) والأدوات الرقمية (الهجمات الإلكترونية، التضليل الإعلامي)، ما يتطلب استجابة متكاملة بنفس القدر.

2- تطور الاستجابة الإستونية: بناء منظومة دفاعية متكاملة

في مقابل هذه التهديدات المتصاعدة، لم تقف إستونيا مكتوفة الأيدي، بل حولت أزماتها المتكررة إلى فرص لتعزيز منظومتها الدفاعية على عدة مستويات:

فعلى المستوى المؤسسي:

لم تكتف إستونيا بإنشاء مركز التميز للدفاع السيبراني (CCDCOE) عام 2008، بل واصلت تطوير مؤسساتها. ففي عام 2021، أنشأت السفارة الإستونية للدفاع مركز CR14 لتقديم التدريب والبحث في الأمن السيبراني للقطاعين العام والخاص على المستويين المحلي والدولي. وفي عام 2023، أطلقت "آلية تالين" (Tallinn Mechanism)، وهي مبادرة دولية لدعم احتياجات أوكرانيا السيبرانية، ما حول إستونيا من متلقية للمساعدة إلى مانحة للخبرة. كما تم إنشاء أول "سفارة بيانات" (Data Embassy) في الخارج، وهي منشأة تستضيف البيانات الحكومية الإستونية بشكل متزامن مع الخوادم المحلية، لضمان استمرار الخدمات الحكومية حتى في حال تعرضت إستونيا لهجوم إلكتروني كبير أو غزو عسكري.[23]

وفي آذار 2024، تم تدشين المبنى الجديد لمركز CCDCOE في تالين باستثمارات بلغت 6.2 مليون يورو، ليصبح المقر الرئيسي لخبراء السيبرانيين من 32 دولة عضو في الناتو و7 دول شريكة غير أعضاء، بما في ذلك أوكرانيا واليابان وكوريا. كما أصبحت قيادة القوات السيبرانية الإستونية (Estonian Cyber Command) تعمل بكامل طاقتها منذ عام 2023، وتتمتع بقدرات هجومية ودفاعية متكاملة.[24]

وعلى المستوى المالي:

رفعت إستونيا الإنفاق الدفاعي بشكل غير مسبوق، حيث قررت رفعه إلى 5% من الناتج المحلي اعتباراً من عام 2026، وإلى 5.4% بحلول عام 2029، وهو من أعلى المعدلات في حلف الناتو. كما أنشأت الحكومة صندوق التكنولوجيا الدفاعية (Defence Tech Fund) بقيمة 100 مليون يورو، بهدف تنمية قطاع التكنولوجيا الدفاعية من حوالي 500 مليون يورو إلى 2 مليار يورو بحلول عام 2030.[25]

وعلى المستوى التكنولوجي والتعليمي:

استثمرت إستونيا في الجيل القادم من خلال برنامج "AI Leap 2025"، الذي يهدف إلى توفير أدوات تعليمية قائمة على الذكاء الاصطناعي مجاناً لنحو 20,000 طالب و3,000 معلم اعتباراً من أيلول 2025. كما تواصل إستونيا تطوير منصة X-Road المفتوحة المصدر التي تتيح للإستونيين الوصول إلى أكثر من 99% من الخدمات العامة عبر الإنترنت. [26]

وأخيراً على المستوى التدريبي والعملياتي:

يواصل تمرين "Locked Shields" – الذي يُعد الأكبر عالمياً في الدفاع السيبراني – تطوره، حيث شارك فيه عام 2025 حوالي 4,000 خبير من 41 دولة. كما أطلقت إستونيا تمرين "Crossed Swords" المتخصص في العمليات السيبرانية الهجومية، وتمرين "Hedgehog 2025" العسكري الضخم الذي شارك فيه 16,000 جندي من قوات الناتو لاختبار الانتشار السريع. وفي كانون الأول 2025، اختتمت في تالين تمرين "Cyber Coalition" التابع لحلف الناتو بمشاركة أكثر من 1,300 مشارك من 29 دولة عضو و7 دول شريكة.[27]

ثالثاً: الدروس المستفادة

قبل استخلاص الدروس، ومن خلال تحليل الجداول السابقة جميعاً تتكشف عدة حقائق استراتيجية، على النحو الآتي:

- تظهر البيانات التكامل العضوي بين الأبعاد المختلفة للهجوم، حيث عمل كل بُعد على تعزيز تأثير الآخر، ما خلق تأثيراً تراكمياً تجاوز مجموع أجزائه.
- يكشف التحليل الكمي الانتقال من نمط "رد الفعل" إلى "الفعل الاستباقي" في استجابة إستونيا، حيث تحولت الأزمة إلى فرصة لبناء مرونة وطنية شاملة.
- تؤكد الأرقام أن نجاح المواجهة لم يكن معتمداً على القوة التقنية فحسب، بل على التكامل بين الآليات الرسمية وغير الرسمية، المحلية والدولية.

هذا التحليل الكمي يثبت أن الحرب الهجينة، رغم تعقيدها، قابلة للقياس والتحليل، وبالتالي يمكن التخطيط لمواجهتها بمنهجية علمية.

كما تشكل الدروس المستفادة من التجربة الإستونية مرجعية أساسية لأي دولة تسعى لتعزيز مرونتها في مواجهة التهديدات الهجينة، على النحو الآتي:

1- على المستوى الاستراتيجي:

- الاعتماد الرقمي كقوة ونقطة ضعف: تثبت الحالة أن التحول الرقمي يخلق نقاط قوة هائلة (كفاءة، شفافية) ولكنه يخلق أيضاً نقاط ضعف استراتيجية. يجب أن تسير استراتيجيات التحول الرقمي يداً بيد مع استراتيجيات الأمن السيبراني.
- ضرورة دمج الأمن السيبراني في صميم الأمن القومي: لم يعد الأمن السيبراني مجرد قضية تقنية، بل أصبح ركيزة أساسية من ركائز الأمن القومي. يجب أن يكون هناك مجلس أمن قومي يدمج ممثلين عن القطاعات السيبرانية والمالية والطاقة.
- أهمية التخطيط الاستباقي ووضع سيناريوهات للطوارئ: كان لاستجابة إستونيا الفعالة جذور في الوعي المسبق باحتمالية التعرض لمثل هذه الهجمات. يجب على الدول تطوير خطط طوارئ وطنية شاملة للتعامل مع الهجمات الهجينة، تشمل جميع القطاعات.

2- على المستوى التشغيلي:

- بناء شراكات فعالة بين القطاعين العام والخاص: كان التعاون بين مركز CERT-EE وشركات الاتصالات والبنوك عاملاً حاسماً في التصدي للهجوم. يجب إنشاء أطر مؤسسية للتنسيق وتبادل المعلومات بين الحكومة والقطاع الخاص الذي يدير معظم البنية التحتية الحيوية.
- تطوير قدرات الاستخبارات الإلكترونية والإنذار المبكر: ضرورة الاستثمار في بناء قدرات استخباراتية قادرة على رصد المؤشرات المبكرة للهجمات الإلكترونية والحملات المعلوماتية، والتنبؤ بها.
- تعزيز المرونة المجتمعية و"المناعة" ضد المعلومات المضللة: تثبت الحالة أن المواطن المستنير هو خط الدفاع الأول. يجب على الدول الاستثمار في محو الأمية الإعلامية والرقمية (Media and Digital Literacy)، وتعزيز الشفافية الحكومية، وبناء قنوات اتصال موثوقة مع الجمهور لمواجهة الشائعات.

3- على المستوى الدولي:

- دور التحالفات الدولية في الردع والاستجابة: كان دعم الناتو عاملاً نفسياً ومادياً بالغ الأهمية لإستونيا. يجب على الدول، وخاصةً الصغيرة منها، تعزيز وجودها في التحالفات الدولية والأطر الأمنية الجماعية التي يمكن أن توفر الدعم السياسي والتقني في أوقات الأزمات.
- السعي لتطوير الأطر القانونية الدولية: كشفت الحالة عن فجوة في القانون الدولي فيما يتعلق بالهجمات الإلكترونية. يجب على الدول العمل معاً لتطوير أطر قانونية وسياسات دولية تحدد قواعد السلوك في الفضاء الإلكتروني وتجعل من الصعب إنكار الهجمات.

الدروس المستفادة من التطور الإستوني (2007–2025):

من خلال تتبع مسار إستونيا منذ 2007 وحتى 2025، يمكن استخلاص دروس إضافية تتجاوز ما تم طرحه سابقاً، على النحو الآتي:

1. المرونة المؤسسية المستدامة: لم تكتف إستونيا برد فعل لحظي على أزمة 2007، بل بنت منظومة مؤسسية (CCDCOE، CERT-EE، CR14، Cyber Command) تطورت وتوسعت باستمرار لتواكب تطور التهديدات. وهذا يؤكد أن بناء المرونة هو عملية مستمرة وليست إنجازاً لمرة واحدة. وهذا يتفق مع دراسة (Schultz, 2025) [28].

2. التحول من الدفاع إلى الريادة: استطاعت إستونيا تحويل موقعها كضحية إلى موقع قيادي عالمي، من خلال استضافة مراكز الخبرة الدولية (CCDCOE) وتصدير خبرتها لدول أخرى مثل أوكرانيا ومولدوفا. هذا يؤكد أن الأزمات يمكن أن تخلق فرصاً استراتيجية إذا ما تمت إدارتها بحكمة.

3. تكامل الأدوات الدفاعية: الجديد في مرحلة ما بعد 2022 هو التكامل بين التهديدات السيبرانية والمادية (قطع الكابلات، انتهاك الأجواء، التخريب الحدودي)، ما يتطلب استجابة متكاملة بنفس القدر، حيث لم تعد الجدران النارية وحدها كافية، بل لا بد من تنسيق وثيق بين الدفاع السيبراني والدفاع التقليدي.

4. الاستثمار في رأس المال البشري: أدركت إستونيا مبكراً أن الأمن السيبراني يبدأ بالتعليم، فاستثمرت في مشروع "Tiger Leap" منذ عام 1997، وتواصل ذلك ببرنامج "AI Leap 2025". هذا يؤكد أن بناء الكفاءات الوطنية هو الاستثمار الأكثر جدوى على المدى الطويل.

5. الردع بالحرمان لا العقاب: يتضح أن زيادة الوجود العسكري لحلف الناتو في المنطقة قد أدت إلى زيادة النشاط الهجين الروسي بدلاً من ردعه. وهذا يشير إلى الحاجة إلى تطوير استراتيجية ردع أكثر شمولاً، تجمع بين الردع بالعقاب والردع بالحرمان.

تقدم الدروس المستفادة من أزمة إستونيا نموذجاً متكاملاً للمرونة في العصر الرقمي. حيث تؤكد أن الدفاع الفعال لا يعتمد على الحلول التقنية فحسب، بل على نسيج استراتيجي يدمج الأمن السيبراني في صميم الأمن القومي، ويبني شراكات عضوية بين القطاعين العام والخاص، وينمي مناعة مجتمعية ضد التضليل. والأهم هو التحول من رد الفعل إلى الاستباقية، ومن الدفاع إلى بناء القدرة على الصمود والتعافي. كما أن التجربة الإستونية تثبت أن التهديد الهجين، رغم خطورته، يمكن أن يخلق تحولاً استراتيجياً إيجابياً يعزز مكانة الدولة وأمنها على المدى الطويل، ما يجعل من الأزمة فرصة للبناء والتطوير.

خاتمة:

تشكل تجربة إستونيا عام 2007 ناقوس خطر استراتيجي ودروساً ملهمة في الوقت ذاته. لقد أثبتت أن ساحات الحرب لم تعد تقتصر على البر والبحر والجو، بل امتدت إلى الفضاء الإلكتروني وعقول الأفراد وقلوبهم. إن الهجوم الهجين الذي تعرضت له هذه الدولة الصغيرة كشف عن وجه جديد للصراع، أكثر خداعاً وتعقيداً، لكنه كشف أيضاً عن أن أساليب المواجهة يجب أن تكون هي الأخرى هجينة، تجمع بين الحزم التقني والحصانة المجتمعية والتعاون الدولي.
الدرس الأعمق الذي تتركه لنا هذه الحالة هو أن المرونة الوطنية هي السلاح الاستراتيجي الأهم في القرن الحادي والعشرين. فهي التي تحدد قدرة الأمم على الصمود والنهوض من جديد. هذه المرونة لا تكمن في الجدران النارية أو أنظمة الدفاع المتطورة فحسب، بل تتجسد في إرادة شعب موحد، ووعي مواطن مسؤول، وثقة بين الحكومة والمحكوم، وشراكات متينة بين جميع مكونات الدولة، وانتماء لتحالفات دولية فاعلة.
لقد حولت إستونيا محنتها إلى منحة، وأدركت أن أفضل دفاع هو بناء مجتمع رقمي متقدم وآمن لا يمكن اختراقه بسهولة. أما بالنسبة للدول النامية، فإن استخلاص العبر من هذه التجربة ليس ترفاً فكرياً، بل هو ضرورة استراتيجية في عالم تتقاطع فيه التحديات وتتصاعد فيه حدة الحرب المعلوماتية والتهديدات السيبرانية. إن بناء مرونة وطنية شاملة هو الاستثمار الأكثر جدوى لضمان الاستقرار والأمن في زمن لا مكان فيه للضعفاء.

النتائج و المناقشة:

أولاً: النتائج

توصل البحث إلى مجموعة من النتائج الرئيسية التي يمكن إجمالها في الآتي:

1. طبيعة الصراع المتغيرة: أكدت حالة إستونيا أن الحروب المستقبلية ستكون هجينة بطبيعتها، تطمس الخطوط بين الحرب والسلم، وتستهدف نقاط الضعف في المجتمعات المفتوحة بأدوات غير مكلفة نسبياً ذات تأثير استراتيجي مدمر.
2. المرونة كاستراتيجية شاملة: نجاح إستونيا لم يكن نتيجة للتفوق التقني فقط، بل كان نتاجاً لمرونة شاملة شملت: الصلابة التقنية، والتماسك الاجتماعي، والمرونة المؤسسية، والدعم الدولي.
3. فشل استراتيجية التقسيم: على الرغم من المحاولات المكثفة لتأجيج الانقسام الإثني داخل إستونيا، فإن الهجوم أدى في النهاية إلى تعزيز التماسك الوطني لدى غالبية الإستونيين، ما يشير إلى أن المجتمعات المتماسكة هي الأقل عرضة للاختراق.
4. تحول التهديد إلى فرصة: استطاعت إستونيا، من خلال الدبلوماسية النشطة والاستثمار الاستراتيجي، تحويل نفسها من ضحية لهجوم سيبراني إلى مركز عالمي رائد في مجال الأمن السيبراني، ما عزز أمنها وحسن صورتها الدولية.

ثانياً: الاستنتاجات و التوصيات:

بناءً على النتائج والدروس المستفادة، يقدم البحث التوصيات الآتية للدول، مع إيلاء اهتمام خاص بالدول النامية:

على المستوى الاستراتيجي الوطني:

1. اعتماد استراتيجية وطنية للمرونة الهجينة: وضع وتنفيذ استراتيجية شاملة لمجابهة التهديدات الهجينة، تدمج فيها جميع الجهود الوطنية (السيبرانية، والإعلامية، والأمنية، والاقتصادية) تحت قيادة موحدة في أعلى مستوى.

2. إدماج الأمن السيبراني في صميم الأمن القومي: إنشاء هيئة أو مركز وطني للأمن السيبراني يتمتع بصلاحيات واسعة للتنسيق والاستجابة للتهديدات، على أن يتبع مباشرة لمجلس الأمن القومي.

3. تعزيز السيادة الرقمية والمعلوماتية: الاستثمار في تطوير بنية تحتية رقمية وطنية آمنة، ودعم وسائل الإعلام المحلية الموثوقة، وتقليل الاعتماد على المنصات الخارجية في أوقات الأزمات.

4. كما يوصي الباحث بإجراء دراسات مستقلة معمقة لتطبيق هذه الدروس في السياقات الوطنية المختلفة، خاصةً في الدول التي تعاني من عقوبات اقتصادية أو إعادة البناء والتنمية، حيث تختلف الظروف والبيانات المتاحة عن حالة إستونيا التي شكلت محور هذا البحث.

على المستوى التكتيكي التشغيلي:

1. بناء شراكات فعالة بين القطاعين العام والخاص: تطوير أطر مؤسسية وقانونية تتيح تبادل المعلومات والإنذارات المبكرة حول التهديدات بين الحكومة ومشغلي البنية التحتية الحيوية في القطاع الخاص (الاتصالات، الطاقة، المال).

2. تطوير قدرات الاستخبارات الإلكترونية: إنشاء وحدات متخصصة في الاستخبارات الإلكترونية قادرة على رصد وتحليل التهديدات والعمليات المعلوماتية المعادية، والتكهن بها.

3. بناء المناعة المجتمعية: إطلاق برامج وطنية لمحو الأمية الإعلامية والرقمية، تهدف إلى تثقيف المواطنين حول كيفية اكتشاف الأخبار المزيفة والدعاية، وتشجيع التفكير النقدي.

على المستوى الدولي والإقليمي:

1. تعزيز التعاون والتحالفات الإقليمية والدولية: العمل على بناء تحالفات إقليمية عربية للتعاون في مجال الأمن السيبراني ومواجهة الحرب المعلوماتية، وتبادل الخبرات والإنذارات.

2. توطين التكنولوجيا والمعرفة: الاستثمار في بناء كفاءات وطنية في مجالات الأمن السيبراني والذكاء الاصطناعي، وتوطين هذه الصناعات الاستراتيجية لتقليل الاعتماد على الخارج.

3. الدبلوماسية الإلكترونية النشطة: تفعيل دور الدبلوماسية العامة والإلكترونية لتقديم الرواية الصحيحة ومواجهة حملات التشويه الدولية، على غرار ما فعلته إستونيا بنجاح.

References:

[1]M. Shady, "Fifth-Generation Wars: Methods of Internal Detonation on the International Scene," (in Arabic) 1st ed., Al-Arabi for Publishing and Distribution, Cairo, Egypt, pp. 1-15, 34, 2019.
[2]F. G. Hoffman, "Hybrid Warfare and Challenges," JFQ: Joint Force Quarterly, vol. 52, no. 1, pp. 34-39, 2009.
[3] O. Fridman, "Russian 'Hybrid Warfare': Resurgence and Politicisation," Oxford University Press, p. 75, 2018.
[4] J. R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," Journal of Cybersecurity, vol. 1, no. 1, pp. 21-37, 2015.
[5] C. Paul, "Strategic Communication: Origins, Concepts, and Core Debates," in Strategic Communication, Praeger, pp. 1-66, 2011.
[6] M. Galeotti, "Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right," Mayak Intelligence, vol. 104, 2016.
[7] A. Rami, "Cybersecurity and Hybrid Warfare," Journal of Technology in Security, (in Arabic) no. 2, p. 67, 2014.
[8] A. Aziz, "The Tactical Dimensions of Hybrid Wars," International Journal of Strategic Thought, no. 3, p. 56, 2016.
[9]B. Mirosław, "How to Understand The Hybrid War?," Securitologia, (in Arabic) no. 1, pp. 27-28, 2015.
[10]F. G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," Potomac Institute for Policy Studies, p. 8, 2007.
[11]H. Mölder and V. Sazonov, "The Bronze Soldier Crisis of 2007: A Case of Hybrid Warfare," Baltic Security & Defence Review, vol. 13, no. 2, pp. 87-112, 2011.
[12] A. Ansip, "Statement by Estonian Prime Minister Andrus Ansip on the relocation of the Bronze Soldier," Government of Estonia Press Office, 2007.
[13] CERT-EE, "Estonian Cyber Attacks 2007: Summary Report," Estonian Information System's Authority, pp. 4-8, 2007.
[14] ECRI, "ECRI Report on Estonia (fourth monitoring cycle)," European Commission against Racism and Intolerance, Council of Europe, pp. 20-25, 2009.
[15]OHCHR, "Report on the events in Tallinn, Estonia, on 26-28 April 2007," Office of the United Nations High Commissioner for Human Rights, pp. 3-6, 2007.
[16]Estonian Ministry of Foreign Affairs, "Statement concerning border delays and economic pressure from Russia," 2007.
[17]The Economist, "Cyberspace: The New Battleground," May 10, 2007.
[18] NATO, "NATO strengthens cooperation with Estonia in cyber defence," NATO Press Release, 2007.
[19]R. Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Proceedings of the 9th European Conference on Information Warfare and Security, pp. 110-115, 2010.
[20] E. Tikk, K. Kaska, and L. Vihul, "International Cyber Incidents: Legal Considerations," NATO CCD COE Publications, p. 78, 2010.
[21]L. Carmichael, "Lessons from small and highly-digitalised Estonia: Decision-making in the aftermath of cybersecurity crises," Internet Policy Review, vol. 14, no. 3, 2025. doi: 10.14763/2025.3.2028
[22] H. Mölder, V. Sazonov, and R. Loik, "Challenges to homeland security in countering latent hybrid threats during the war in Ukraine: The case of Estonia," in Russian Influence

Operations and the War in Ukraine, Springer, pp. 235-260, 2025. doi: 10.1007/978-3-032-01461-0_10

[23]Estonian Government, "Data Embassy: Securing Government Data in the Cloud," 2023.

[24] Defence24, "Development of Cyber Forces in NATO Countries," September 27, 2025.

[25] Estonian Government, "DefenceTech Fund: 100 Million Euros for Defence Technology," 2024.

[26]Großwald European Defence Intelligence, "Estonia's Cyber Fortress: Securing Nations in the Digital Era," December 3, 2024.

[27] NATO, "Cyber Coalition 2025 Exercise Concludes in Tallinn," December 2025.

[28] D. Schultz, R. Smaliukiene, and V. Giedraityte, Eds., "Democratic Resilience in the Baltics, Vol. 1: Resilient Governance and Democratic Stability," Springer Nature, 2025. doi: 10.1007/978-3-031-99286-5