٢٠

مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

# دراسات

## الحرب تحت مسمى جديد: الاختراق الروسي لأجهزة الحاسبات الآلية في الولايات المتحدة الأمريكية والغرب

جمادى الأولى ١٤٣٨هـ/ فبراير ٢٠١٧م

جاك كارافيللي سيباستيان ماير

ترجمة:
عبدالعزيز الحميد

# الحرب تحت مسمى جديد:
# الاختراق الروسي لأجهزة الحاسبات الآلية في الولايات المتحدة الأمريكية والغرب

جاك كارافيللي سيباستيان ماير

ترجمة:
عبدالعزيز الحميد

ح مركز الملك فيصل للبحوث والدراسات الإسلامية، ١٤٣٨هـ

*فهرسة مكتبة الملك فهد الوطنية أثناء النشر*

كارافيللي، جاك

الحرب تحت مسمى جديد: الاختراق الروسي لأجهزة الحاسبات الآلية في الولايات المتحدة الأمريكية والغرب./ جاك كارافيللي؛ سيباستيان ماير؛ عبدالعزيز الحميد.- الرياض، ١٤٣٩هـ.

٣٢ ص؛ ١٦,٥X ٢٣ سم .- (دراسات ٢٠)

ردمك: ٦-٤١-٨٢٠٦-٦٠٣-٩٧٨

١- روسيا – العلاقات الخارجية – الولايات المتحدة ٢- الحرب الإلكترونية أ. ماير، سيباستيان (مؤلف مشارك) ب. الحميد، عبدالعزيز (مترجم) ج. العنوان د. السلسلة

ديوي ٣٢٧,٧٣٠٤٧ ١٤٣٩/٢٥٤٩

**رقم الإيداع: ١٤٣٩/٢٥٤٩**

**ردمك: ٦-٤١-٨٢٠٦-٦٠٣-٩٧٨**

---

**تحرير ومراجعة**

يوسف حجاج

**تصميم وإخراج**

محمد يوسف شريف

## إخلاء مسؤولية

تعكس هذه الدراسة ومحتوياتها تحليلات الكاتب وآراءه، ولا ينبغي أن تُنسب وجهات النظر والآراء الواردة فيها إلى مركز الملك فيصل للبحوث والدراسات الإسلامية، والكاتب وحده هو المسؤول عما يرد فيها من استنتاجات أو إحصاءات أو أخطاء.

# المحتويات


| | |
|---|---|
| تمهيد | ٦ |
| مخاطر متنامية | ٦ |
| الحرب المعلوماتية تستعر | ٩ |
| بين التكنولوجيا والسياسة | ١٢ |
| سنودن.. صداع في رأس السلطة | ١٣ |
| تقاعس يكشف أسرارًا | ١٦ |
| انتخابات في مهب الريح | ١٩ |
| عقوبات غير مجدية | ٢١ |
| الخاتمة | ٢٧ |

## تمهيد

جاء تطوُّر شبكة الإنترنت والحاسبات الآلية التي تواكبها إنجازاً علمياً عظيماً للبشرية. وشَكَّلَ الاثنان معاً ما عُرف بالفضاء الإلكتروني؛ أي «مملكة شبكات الحاسبات الآلية، ومن يستخدمونها، والتي يتم من خلالها تخزين المعلومات ومشاركتها وتداولها على الإنترنت»[١].

وتتوارى خلف هذا التعريف سلسلة غير متناهية من الأنشطة اليومية العالمية على الإنترنت، التي يمكن أن تشمل أموراً متعددة، تبدأ من إرسال تهنئة بسيطة إلى أحد الأصدقاء في مكان ما من العالم بمناسبة ذكرى ميلاده، أو تبادل الشركات والمراكز العلاجية البيانات مع نظيراتها، ولا تنتهي بالحوارات القائمة داخل الحكومات أو بين بعضها بعضاً؛ فقد كان الهدف الأساسي من اختراع الإنترنت وتطويرها أن تكون مجانيةً وفي متناول الجميع؛ إذ كان مخترعوها يأملون في أن يتمكن العلم من خدمة البشرية بتيسير الوصول إلى المعلومات.

تحقَّقَ هذا الهدف النبيل والمثالي في صور شتى، من بينها الأمثلة المذكورة هنا؛ فالإنترنت، هي بكل المقاييس، تطور مذهل يحفز الرخاء العالمي. لكنَّ هذا ليس كل ما في الأمر؛ فالإنترنت مهَّدت الطريق - في الوقت نفسه - لواقع أكثر قُبحاً؛ فالمجرمون على شبكة الإنترنت يرتكبون الكثير من الجرائم الإلكترونية، مثل: سرقة بيانات الملكية؛ ليحققوا من خلالها مكاسب مالية ضخمة، كما أن المنظمات الإرهابية (مثل: تنظيم داعش) تستخدم الإنترنت وسيلةً لترويج أفكارها العنيفة، وتشجيع أتباعها، وجذب أنصار جُدد.

## مخاطر متنامية

ومن المخاطر المتنامية أيضاً لسوء استعمال الإنترنت: استخدام كثير من الدول لها لتحقيق أهدافها السياسية؛ فنجد كلاً من الصين، وكوريا الشمالية، وإيران - مثلاً - أتقنت استخدام الإنترنت بطرائق تُمكِّنها من تعزيز غاياتها السياسية لتعطيل أعدائها، وتقويض الحكومات المعارضة. وقد استطاعت الصين الاستيلاء على الملفات الخاصة

(1) P. W. Singer and Allan Friedman, *Cybersecurity and Cyber Warfare: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 13.

باثنين وعشرين مليون مواطن أمريكي، شغلوا وظائف متعددة في الحكومة الأمريكية، من قسم إدارة شؤون الأفراد الأمريكية.

وقد تكون الحكومة الروسية، ومَنْ يعملون نيابةً عنها، أكثر الحكومات التي استخدمت الإنترنت بشكل أكثر ابتكاراً لتحقيق أغراض سياسية؛ فالجرائم الإلكترونية الروسية ضد الغرب مستمرة وفاعلة ومتنامية، من حيث نطاقها وطبيعتها، وهي موجهةٌ غالباً إلى الولايات المتحدة الأمريكية. كما أن الهجمات الإلكترونية يمكن أن تكون مدمِّرةً كالهجمات الحركية، ولكن بأشكال مختلفة تماماً.

سعى الاتحاد السوفيتي، ثم روسيا، خلال النصف الأخير من القرن العشرين، وتحديداً منذ نهاية الحرب العالمية الثانية، إلى استخدام الدعاية والتقنيات ذات الصلة للتأثير في دول أخرى أو التفوق عليها. ومن المؤكد أن استخدام روسيا الإنترنت لتنفيذ هجمات إلكترونية أمر حديث نسبياً، لكنَّ هجومها الإعلامي لا يزال ممتداً على مدار عقود.

وقد أدى انهيار الاتحاد السوفيتي عام ١٩٩١م إلى تراجع حادٍّ للعسكرية الروسية. كما تزامن الانهيار السياسي مع الانهيار المالي، وظل الجيش الروسي يعاني مدة طويلة من الحاجة الماسة إلى الدعم المالي. وحينئذ؛ رأى كبار القادة العسكريين أن الحروب المعلوماتية والعمليات الإلكترونية وتكاليفها المنخفضة نسبياً قد تكون وسيلةً للتعويض عن أوجه القصور المتنامية في القدرات القتالية الأخرى.

وفي الوقت نفسه، قام الخبراء الاستراتيـجيون في الجيش الروسي، الذين كانوا حريصين دوماً على معرفة ما يقوم به أعداؤهم، بدراسة أهمية عمليات الحرب الإلكترونية التي أجرتها الولايات المتحدة الأمريكية عام ١٩٩١م لإخراج القوات العراقية التابعة لصدام حسين من الكويت. وقد ترتب على هذه الدراسة الاعترافُ بتقدُّم الولايات المتحدة الأمريكية في مجال الحروب الإلكترونية، وحاجة الجيش الروسي إلى أن تتبنَّى روسيا برنامجاً لامتلاك مجموعة من القدرات القوية المتعلقة بالحرب الإلكترونية.

لم تحدث هذه التطورات بين عشيةٍ وضحاها، وإنما ظهرت تباعاً؛ ففي عام ١٩٩٨م، قام مكتب التحقيقات الفيدرالية الأمريكي بإجراء تحقيقات عُرِفت باسم (عملية متاهة ضوء القمر) كردٍّ فعلٍ على سلسلة من محاولات اختراق أجهزة الحاسب الآلي؛ حيث يتم حفظ المعلومات السرية الخاصة بتكنولوجيا سلاح الطيران الأمريكي، وتحديداً المعلومات

المحفوظة في قاعدة (رايت بـاترسون) الجوية الموجودة في مدينة آكرون في ولاية أوهايو، وهي أحد أهم مراكز البحث والتطوير التابعة للقوات الجوية. كما كانت هناك هجمات على شبكات الحاسب الخاصة بأهم مرافق الأسلحة النووية الموجودة في معمل (ساندیا) القومي، ومعمل (لوس آلاموس) القومي، الموجودين في ولاية نيومكسيكو.

وقد أسفر التحقيق عن عدة نتائج، منها: أنه تمت سرقة آلاف الصفحات والوثائق، وأن عمليات الاختراق شملت دولاً أخرى، مثل: ألمانيا، والمملكة المتحدة، وكندا، والبرازيل. وليست هذه المرة الأولى التي تقع فيها ألمانيا ضحيةً لعمليات الاختراق الإلكتروني؛ ففي ثمانينيات القرن العشرين قام مواطن ألماني يُدعى ماركوس هيس ببيع كثير من الأسرار الألمانية إلى روسيا. وقد أكدت هذه الواقعة أهمية تحديد المخاطر الداخلية. وقد وجدت المباحث الفيدرالية أن أربعة عناوين إلكترونية مصدرها روسيا متورطة في الهجمات التي تمت في أواخر تسعينيات القرن العشرين الميلادي، مع أن روسيا لم تعترف بتورُّطها في أيٍّ منها.

وفي عام ٢٠٠٧م شرعت روسيا في القيام بهجمات استهدفت بعض البلدان الغربية، ومنها: أستونيا، وليتوانيا، وبولندا، وجورجيا. فعلى سبيل المثال قام قراصنة الإنترنت في شهري أبريل ومايو عام ٢٠٠٧م بشنِّ هجمات إلكترونية على الحكومة الأستونية والمؤسسات المالية؛ انتقاماً من قرار أستونيا إزالة النُّصب التذكاري الروسي الخاص بالحرب العالمية الثانية. وفي العام التالي (٢٠٠٨م)، وانتقاماً من «جرائم» مماثلة، تم تشويه الموقع الخاص بالحكومة الليتوانية وإدراج رمزي المطرقة والمنجل الروسيين في الموقع.

لم يكن ذلك مفاجئاً للمراقبين الفطنين من أمثال مايكل ماكفول، أحد سفراء الولايات المتحدة السابقين إلى روسيا؛ فقد صرَّح منذ عدة سنوات مضت قائلاً: «لسنوات، والكرملين يبحث عن سُبل لعرقلة الأنظمة الديمقراطية ومساعدة من يروق له من الشعوب للوصول إلى السلطة وتقويض مصداقية العملية الديمقراطية»[٢].

ولا شك في أن تلك الهجمات، وما تلاها من هجمات إلكترونية روسية على أهداف أكثر أهمية، مثل: الولايات المتحدة الأمريكية، وألمانيا يمكن أن تُعزى إلى إجراءات رسمية. وقد

(٢) انظر:
"The Key to Putin's Cyber Power," *The Atlantic*, December 30, 2016; interview with Uri Friedman.

حافظت كل من مديرية المخابرات الرئيسية (GRU)، وخدمة الأمن الاتحادية (FSB) – التي خلفت لجنة أمن الدولة (KGB) المعروفة للجميع – على كوادر متخصصة ومتفانية من خبراء الإنترنت[٣]. كما يأتي – على القدر نفسه من الأهمية – ما يقوم به جهاز المخابرات الخارجية (SVR) من مراقبة للإعلام والمدوِّنين في الغرب؛ من أجل الحصول على مزيد من المعلومات التي يمكن استخدامها أو تشويهها لصالح الأغراض السياسية الروسية.

وفي أواخر عام ٢٠١٦م صدر تقرير مشترك عن إدارة الأمن القومي (DHS) ومكتب التحقيقات الفيدرالية (FBI) بالولايات المتحدة الأمريكية، بعنوان (السهوب الرمادية: النشاط الإلكتروني للبرمجيات الروسية الضارة)، تم من خلاله تحديد الهيئات الحكومية الروسية المتورطة بشكل مباشر في شنِّ هجمات إلكترونية على البنية التحتية الحيوية في الولايات المتحدة الأمريكية. وقد نُصِحَت الشركات الأمريكية بإشعار مسؤولي الحكومة إذا ارتابوا في وجود أي هجمات إلكترونية على أجهزة الحاسب الآلي الخاصة بهم. وشمل التقرير أيضاً المؤسسات الأخرى التي هي عُرضة لهذه الهجمات، مثل: الجامعات، والمراكز الفكرية، ومواقع البنية التحتية المهمة، والهيئات السياسية. وكما هو متوقع؛ أنكرت الحكومة الروسية جميع هذه الاتهامات مستخدمة أوصافاً من قبيل: «هيستيريا»، و«لا أساس لها من الصحة»؛ لوصف ما جاء في التقرير[٤].

## الحرب المعلوماتية تستعر

وعلى الرغم من أهمية هذا التقرير في تحديد أنشطة روسيا الإلكترونية؛ إلا أنه عجز عن مواجهة الخطر الذي يتعرَّض له الأمن القومي للولايات المتحدة الأمريكية في الخارج؛ أي الحرب المعلوماتية. وفي أفغانستان لا تزال الولايات المتحدة تقاتل عدواً متجدداً لا يفتر عزمه منذ عام ٢٠٠١م، هو (طالبان). وقد كلفت هذه الحرب، التي طال أمدها، الولايات المتحدة الآلاف من الأرواح، وأكثر من تريليون دولار.

(٣) حوار مع الضابط السابق في سي آي إيه: بيتر براي، في ٨ فبراير ٢٠١٧م، في واشنطن العاصمة.

(٤) أحد أفضل التقييمات التي تم تقديمها حول هذا التقرير ذلك الذي قدمه (فيل نيراي) بعنوان:
"DHS/FBI Report Confirms Russian Cyber Units Attacked Critical Infrastructure with Malware," https://cyberx-labs.com/en/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/.

وفي شهادة استماع أمام لجنة الخدمات المسلحة في مجلس الشيوخ، في أوائل فبراير ٢٠١٧م، صرَّح الجنرال جون نيكلسون قائد القوات الدولية الأمريكية في أفغانستان، بأن روسيا تستخدم الإنترنت لنشر روايات كاذبة بأن حركة طالبان تقاتل تنظيم (داعش) الإرهابي، بينما لا تقوم القوات الحكومية الأفغانية بذلك. ويدَّعي نيكلسون أن الهدف الروسي لم يكن سوى تقويض جهود الولايات المتحدة الأمريكية وحلف شمال الأطلسي المعاديين لتنظيمي (داعش) و(طالبان)(٥).

وفي ظل تقرير إدارة الأمن القومي ومكتب التحقيقات الفيدرالية وشهادة نيكلسون، فضلاً عن تاريخ روسيا الطويل في الحرب المعلوماتية؛ فإن الإنكار الروسي لا يحمل سوى قدر ضئيل من الحقيقة يصعُب قبوله، كما أن محاولات روسيا التدخل في الانتخابات الرئاسية الأمريكية - وهو ما سنناقشه لاحقاً - تجعل الإنكار الروسي يبدو غير منطقي.

وقد قوَّض كبار المسؤولين الروس بأنفسهم ادِّعاء براءتهم من خلال شنِّ مختلف أشكال الهجمات الإلكترونية. ومن أفضل الأمثلة على ذلك: الحوار الذي أجراه فاليري غيراسيموف القائد العسكري رئيس هيئة الأركان العامة للقوات المسلحة الروسية عام ٢٠١٣م؛ فقد صرح الـجنرال - من خلال ما عُرِف لاحقاً بعقيدة غيراسيموف العسكرية - بأن الخطوط الفاصلة بين الحرب والسلام لم تعد واضحة، وأن التكتيكات السرية، مثل: الحرب المعلوماتية أصبحت ذات أهمية قصوى للنجاح العسكري. ووفقاً لغيراسيموف فإن «قواعد الحرب تغيرت، ونما الدور غير العسكري كوسيلة لتحقيق الأهداف السياسية والاستراتيـجية، وتجاوز، في كثير من الأحوال، في تأثيره وفاعليته قوة الأسلحة». وأطلق عليها «الحرب غير الخطية»(٦). أما في الغرب فيُعرف ذلك بحرب المعلومات.

وفي الآونة الأخيرة انعكست الأهمية القصوى التي توليها المؤسسة العسكرية الروسية للحرب المعلوماتية في تصريحات وزير الدفاع الروسي سيرغي شويغو بأن المؤسسة العسكرية الروسية تقوم حالياً بإنشاء وحدة جديدة للحرب الإلكترونية قوامها ألف موظف، وتحمل اسم (kibervoyska). وسيُوكل إلى هذه الوحدة تطوير كفاءة عمليات

(5) Michael Gordon, "General Seeks More Troops in Afghan 'Stalemate.'" *New York Times*, February 10, 2017, A3.

(6) Neray, "DHS/FBI Report."

الحرب الإلكترونية الروسية. كما ترى المؤسسة العسكرية الروسية أنها تحمي العمليات والمراسلات الإلكترونية الوطنية من أي جهود ترمي إلى تعطيلها.

ويجدر بنا في هذا السياق أن ندرس بإيجاز ما يدفع روسيا إلى هذا الاستخدام العدواني للحرب المعلوماتية؛ فالهدف، في المقام الأول، هو تقويض الديمقراطيات الغربية ومؤسساتها العسكرية، والتأثير في اختيار القادة القوميين الذين يميلون إلى التعاون مع روسيا. ويهدف الرئيس فلاديمير بوتين من هذا إلى مدِّ نفوذ روسيا من المحيط الأطلسي إلى المحيط الهادئ. وفي عام ١٩٩٩م أصدر بوتين تقريراً بعنوان (روسيا في مستهل الألفية) حدَّد فيه ملامح رؤيته لكيفية ظهور روسيا قوةً عظمى على الساحة العالمية في العقود الأولى من القرن الحادي والعشرين. وإذا كان هذا التقييم للدوافع الروسية دقيقاً؛ فمعناه أنه في إطار استخدام الحرب المعلوماتية فإن هناك احتمالاً ضئيلاً لأي قدر من التنازلات، أو الانفراج مع روسيا خلال السنوات المُقبلة.

وهناك عنصر آخر ذو أهمية يتعلق بالدوافع الروسية وراء القيام بعمليات افتراضية؛ فالحكومة الروسية - مثلها مثل جميع الأنظمة الاستبدادية - في ظل قيادة بوتين (ضابط المخابرات الأسبق) ترى نفسها محاطة بالأعداء. وفي حالة روسيا تأتي الولايات المتحدة الأمريكية على رأس قائمة أعدائها الذين يسعون للسيطرة على الساحة العالمية. والبقاء في السلطة أمر ذو أهمية قصوى للأنظمة الاستبدادية؛ بما فيها روسيا تحت قيادة بوتين. ويؤدي ذلك بدوره إلى أن ترى روسيا نفسها في حالة تنافس مستمر، إن لم يكن صراعاً، مع الولايات المتحدة الأمريكية وحلفائها في الغرب؛ فالأيديولوجية الغربية المتمثلة، بشكل أساسي، في الليبرالية والاهتمام بالفرد على حساب الدولة هي نفسها التي دمَّرت الشيوعية.

ومن منظور حيادي؛ فإن جميع هذه التصورات ليست سوى سلسلة من الافتراضات التي لا أساس لها من الصحة؛ فالقادة في الغرب - بوجه عام - لا يرون أنفسهم محاصرين في صراع قاتل مع روسيا؛ بل يرون أن روسيا، وليس الغرب، هي المعتدي في المقام الأول، من خلال تصرفات، مثل: ضم القِرم في مارس ٢٠١٤م، ما يُعَدُّ انتهاكاً لمعاهدة الحدِّ من انتشار الأسلحة النووية متوسطة المدى، بالإضافة إلى الهجمات الإلكترونية وأساليب الحرب المعلوماتية التي لا حصر لها. فهل يعتقد أيٌّ من أعضاء الكرملين الروسي،

أو المؤسسة العسكرية الروسية، أن حلف (الناتو) سيقوم بغزو روسيا، أو أن هناك خطة للإطاحة بالحكومة الروسية؟ أما عن انهيار الاتحاد السوفيتي فستظل روسيا وحكومتها مسؤولتين عن مصير الأمة.

### بين التكنولوجيا والسياسة

إن تداول سيناريوهات غير معقولة، إلى حد كبير، قد يحشد الدعم المحلي من الجمهور الروسي ضعيف الوعي لصالح بوتين، ولكن لا يوجد أساس واقعي يمكن من خلاله استنتاج أن الغرب يرى نفسه عدواً لروسيا. إلا أن هذا لا يعني إنكار وجود فروق شاسعة؛ فهي بالقطع موجودة، غير أن هذه الفروق لا تتضح في الخُطط المُعدَّة لمواجهة المؤسسة العسكرية الروسية؛ بل العكس هو الصحيح؛ إذ إن غالبية الحكومات الغربية، بدايةً من الحكومة الأمريكية الجديدة بقيادة دونالد ترامب، تفضل أن تتحسَّن العلاقات مع روسيا، لكنَّ الخبراء الاستراتيـجيين الروس يخشون المجهول، والسياسات الدولية تحمل في طياتها كثيراً من التحديات المجهولة والمُربكة.

ومن الأمثلة الجيدة على ذلك: الثورات الملوَّنة؛ بما فيها الانتفاضات التي حدثت على مدار العِقد الماضي في أوكرانيا وجورجيا. وهذه الانتفاضات السياسية مُلِهمة للمواطن العادي، كما يمكن أن تحفز التغيير السياسي الذي تخشاه السلطات الروسية.

فمن ناحية، يُعَدُّ استخدام روسيا للهجمات الإلكترونية على الولايات المتحدة الأمريكية تطوراً للتداخل بين التكنولوجيا والسياسة. وقد جعلت المهارات والقدرات الإلكترونية المستمرة في التطور تنفيذ هذه الهجمات أكثر سهولةً، على الأقل بالنسبة إلى عدد قليل من الدول المتطورة تقنياً، مثل روسيا. وعلى ما يبدو أن هذه الظاهرة مستمرة.

اتخذت الولايات المتحدة سلسلة من الإجراءات لحماية مصالحها وأصولها من الهجمات الإلكترونية الروسية والدول الأخرى المُعادية لها، كان من أهمها: إنشاء وحدة القيادة الإلكترونية الأمريكية عام ٢٠٠٩م، التي تقع في جورج ميدفورت في مريلاند. ويشغل الأدميرال مايك روجرز منصب رئيس هذه الوحدة، إضافة إلى شغله منصب مدير وكالة الأمن القومي، وهي أهم مؤسسة حكومية مسؤولة عن جميع العمليات الإلكترونية؛ بما في ذلك الإشارات الاستخباراتية والهجمات الإلكترونية ووسائل الدفاع ضدها.

ولا شك في أن القوات المسلحة الأمريكية والمؤسسات القومية الأمنية والمدنية، مثل: وكالة الاستخبارات المركزية (CIA)، ووزارة الأمن الداخلي (DHS) مُعدَّة حالياً بشكل أفضل مما مضى للعمل في بيئة إلكترونية مُعادية، مثل روسيا؛ إلا أن الولايات المتحدة تعاني مشكلتين أُخريين في محاولاتها منع الدول الأخرى من إحداث أضرار جسيمة من خلال الهجمات الإلكترونية.

أولاهما: عند النظر إلى حجم الحكومة الأمريكية وتعقُّدها؛ فإنه من المستحيل أن تقوم بحماية آلاف الأهداف من الهجمات الإلكترونية، كما أنها ربما لا تستطيع أن تقوم بحماية أهم أهدافها وأكثرها حيوية، التي تُعرف عموماً بالبنية التحتية الأساسية.

ثانياً: من ضمن أوجه القصور الأخرى، إخفاق كثير من الهيئات الحكومية وشركات الأعمال الكبيرة والصغيرة في تدريب العاملين فيها على ما يُعرف بـ(الوعي الإلكتروني)؛ الذي يشمل استخدام الإجراءات المُلائمة للحدِّ من احتمالات تلقِّي الهجمات الإلكترونية. كما تفتقر كثير من هذه المؤسسات والشركات إلى خطط للتعافي من الآثار الناجمة عن الهجمات الإلكترونية أو الحدِّ منها. كما أن هذا قد يزيد في احتمال أن يظل أثر الهجمات الإلكترونية مستمراً، وأن يُوقع أقصى الضرر على الجهة المستهدَفة. وقد تحدَّث ليون بانيتا وزير الدفاع الأمريكي الأسبق ومدير وكالة الاستخبارات المركزية عن (بيرل هاربور الإلكترونية)، في إشارة منه إلى الهجمات الإلكترونية الخطيرة، مثل: محاولة العدو إيقاف شبكة الكهرباء الوطنية أو الاتصالات الخلوية.

### سنودن.. صداع في رأس السلطة

أما المشكلة الأخرى التي تواجهها الولايات المتحدة الأمريكية - ضمن جهودها لدفع الهجمات الإلكترونية - فهي الأضرار الاستثنائية الناجمة عن تصرفات إدوارد سنودن؛ فقد كان سنودن موظفاً شاباً في وكالة الاستخبارات المركزية يعيش في هاواي ويعمل مقاولاً بمؤسسة بوز آلين الدفاعية، وهي إحدى مؤسسات الدفاع الكبرى الموجودة في واشنطن والداعمة لوكالة الأمن الوطني.

أتاحت هذه الوظائف لسنودن أن يتوصل - بشكل استثنائي بصفته مسؤول أنظمة - إلى عدد لا يُحصى من برامج المراقبة الإلكترونية الحساسة التي تستخدمها الحكومة

الأمريكية، المحلية منها والأجنبية. كما استطاع - من خلال منصبه - الحصول بشكل غير مشروع على الآلاف من الوثائق السرية للغاية التي توضح نطاق هذه البرامج وطبيعتها، وقام في عام ٢٠١٣م بنشرها بواسطة فريق من الصحفيين يرأسه جلين جرينولد. تسبَّب نشر هذه الوثائق في الكشف عن فضائح وحدوث ضجة في أنحاء الولايات المتحدة الأمريكية، وسبَّب حرجاً للحكومة الأمريكية عندما كشفت الوثائق أن وكالة الأمن الوطني سجَّلت مكالمات هاتفية للمستشارة الألمانية أنـجيلا ميركل.

أجبرت سنودن تصرفاتُه على مغادرة الولايات المتحدة الأمريكية؛ فهرب أولاً إلى هونج كونج، لكنه سرعان ما اتخذ طريقه إلى موسكو؛ بعدما مُنِح تصريحاً بالبقاء في البلاد. ولديه حالياً تصريح بالإقامة هناك حتى عام ٢٠٢٠م. ويواجه سنودن اتهامات بانتهاك قانون التجسُّس الأمريكي لعام ١٩١٧م، وسرقة ممتلكات حكومية. إضافة إلى ذلك، ولأن حكومة الولايات المتحدة تتعاون في مسائل التجسُّس مع حكومات أجنبية بعينها؛ يُعتقد أن سنودن توصَّل إلى عشرات الآلاف من الملفات التي تسيطر عليها الحكومتان البريطانية والأسترالية.

وما دام سنودن في روسيا؛ فإنه سيبقى بعيداً عن متناول القانون الأمريكي. ومن الأمور الداعية إلى لإحباط أيضاً للحكومة الأمريكية عدم التأكد من كمِّ المعلومات التي كشفها سنودن للروس في مقابل السماح له بالعيش مع صديقته هناك. ولكن من المؤكد أنه تم استجوابه من قِبَلِ مكتب التحقيقات الفيدرالية ومديرية المخابرات الرئيسية، ومن المنطقي أن نفترض، على الرغم من إنكاره، أن روسيا حصلت على قدر لا بأس به من المعلومات عن مصادر وطرائق المراقبة الأمريكية. وقد أطلق بعضهم على سنودن لقب «الوطني»، بينما وصمته حكومة ترامب بالخائن.

كان المشهد الـجيوسياسي هو المحفز الرئيسي وراء الأنشطة الإلكترونية الروسية ضد الولايات المتحدة الأمريكية. وقد ظلت العلاقات الروسية الأمريكية تزداد سوءاً لبعض الوقت؛ خصوصاً بعد انهيار محاولات الرئيس السابق باراك أوباما ووزيرة خارجيته هيلاري كلينتون «إعادةَ ضبطِ» العلاقات مع (الكرملين)، التي استمرت عدة سنوات، في أعقاب قيام روسيا بالضمِّ غير الشرعي للقرم في مارس ٢٠١٤م. وقد أعقب هذا الضمَّ سلسلةٌ واسعةٌ من إجراءات الحظر الأمريكية والغربية ضد الأفراد والمؤسسات

الروسية؛ ما استدعى مزيداً من الأنشطة العدائية الروسية ضد التحالف الغربي. كما قام الجيش الروسي عام ٢٠١٥م بالتدخل في سوريا لدعم الرئيس السوري بشار الأسد ونظامه الإجرامي، وهو التدخل الأول من نوعه في المنطقة منذ سبعينيات القرن الميلادي الماضي.

ولم يكن فلاديمير بوتين يُكنُّ لباراك أوباما سوى قدر ضئيل من الاحترام، وكان هذا الشعور متبادلاً بينهما، ويبدو أن الرئيس الروسي كان يُضمِر كذلك قدراً من العداء لهيلاري كلينتون؛ التي كان يعدُّها مسؤولةً عن التحريض على المظاهرات الروسية عام ٢٠١١م ضد حملة إعادة انتخابه للرئاسة الروسية. لكن لا يوجد دليل يدعم هذه الفكرة.

وعلى الرغم من انزعاج بوتين وشعوره بالحرج إزاء هذه المظاهرات، إلا أنه لم تكن لديه مشكلة في الفوز بفترة رئاسية ثانية في ظل النظام الروسي الديمقراطي الصامت، غير أن فوزه لم يقلل من حنقه على الوزيرة الأمريكية. ومن المفارقات أيضاً أن الرئيس الروسي ينكر بشدة ما يُدَّعي أن كلينتون قامت به؛ نظراً إلى جهود بلده الموثقة تماماً في تقويض العملية الانتخابية في أمريكا وأماكن أخرى.

ومن الجدير بالذكر أن الانتخابات الرئاسية التي تم إجراؤها في نوفمبر ٢٠١٦م كانت واحدة من أقسى التجارب وأكثرها إثارةً للشقاق والخلافات في تاريخ الأمة الأمريكية. كما أنها كانت من أكثرها إثارةً للدهشة؛ فقد استطاع دونالد ترامب، رجل الأعمال الثري المقيم في نيويورك، ذو الأسلوب الحاد، والذي يفتقر إلى الخبرة السياسية، اكتساح عدد كبير من المنافسين؛ ليصبح مرشح الحزب الجمهوري. وكان منافساً ضد مُرشحة الحزب الديمقراطي هيلاري كلينتون، وهي واحدة من أكثر الرموز السياسية شهرةً في الولايات المتحدة الأمريكية؛ إذ إنها كانت عضواً سابقاً بمجلس الشيوخ، وشغلت منصب وزيرة الخارجية الأمريكية، كما أنها زوجة الرئيس الأمريكي الأسبق بيل كلينتون، أحد رجال السياسة المخضرمين بالولايات المتحدة الأمريكية.

وقد ساعدت خبرة كلينتون وتجربتها في جمع الكثير من الأموال؛ ما دفع الكثيرين إلى الظن باستحالة أن يتغلب ترامب عليها. وعلى مدار الحملة كانت هذه الميزات ظاهرة في الاستطلاعات التي توضح أن الغلبة ستكون لكلينتون على ترامب. ولكل هذه الأسباب؛ اعتبرت وسائل الإعلام الأمريكية أن كلينتون هي المرشح الفائز المُحتمل. كما أسهمت

كلينتون بنفسها في تعزيز هذه الفكرة، ولم تقم بالدعاية بشكل قوي في الولايات الأساسية كما فعل ترامب. ولم يكن احتمال فوزها يروق (الكرملين) الذي لم ينسَ دعم كلينتون لمعارضي بوتين. كانت النتيجة أن الانتخابات الرئاسية في الولايات المتحدة عام ٢٠١٦م أصبحت المؤشر على الاستخدام الأكثر وضوحاً وغير المسبوق للإنترنت، وغيرها من وسائل ممارسة روسيا نفوذها ضد الولايات المتحدة، أو أي دولة غربية أخرى مقارنةً بأي وقت مضى. كما أتاحت هذه الحملة الانتخابية الطويلة فرصة مهمة للثأر من هيلاري كلينتون.

في سبتمبر ٢٠١٥م تواصل العميل الخاص في مكتب التحقيقات الفيدرالية أدريان هوكينز مع اللجنة الوطنية الديمقراطية بشأن معلومات غير مؤكدة عن احتمال وجود اختراق كبير لشبكة الحاسب الآلي الخاصة باللجنة. ويعتقد هوكينز أن هذا النشاط مرتبط بمجموعة (الدوقات) -إحدى مجموعات الحاسب الآلي المرتبطة بالحكومة الروسية -، التي ظل مكتب التحقيقات الفيدرالية يراقبها مدة سنتين على الأقل، معتقداً أنها مصدر الهجمات على ملفات الحاسب غير السرية الخاصة بوزارة الخارجية الأمريكية وهيئة الأركان المشتركة التابعة لوزارة الدفاع الأمريكية.

## تقاعس يكشف أسرارًا

كانت الملفات التابعة للجنة الوطنية الديمقراطية مهيأة للاختراق. وهذه اللجنة هي مؤسسة غير ربحية، ولم تُخصِّص موارد كافية لتثبيت وسائل الدفاع الأكثر تطوراً ضد الهجمات الإلكترونية. كما كانت هناك مشكلات مع طاقم العمل؛ فقد أُحيل هوكينز إلى أحد مكاتب المساعدة الذي يعمل فيه موظف بنصف دوام من شيكاغو يُدعى يارد تامين. وقد أثار الموظف شكوك هوكينز، الذي ظن أنه يقوم باتصالات مزيفة، لكنه لم يكن يفعل؛ بل قام بدلاً من ذلك بإجراء فحص سريع لملفات اللجنة الوطنية الديمقراطية، ولم يجد خطأ. وكان تخاذله وفشله في تحليل المعلومات أحد الأسباب المتعددة وراء استمرار عمليات الاختراق مدة سبعة أشهُر من دون انقطاع ومن دون تقصٍّ. ولم يساعد اللجنة الوطنية الديمقراطية عدم قيام العميل الفيدرالي هوكينز بزيارة مقر اللجنة لشرح الموقف، واعتمد بدلاً من ذلك على المكالمات الهاتفية حتى تم اللقاء أخيراً بعد عدة أشهُر بين المسؤولين في مكتب التحقيقات الفيدرالية واللجنة الوطنية الديمقراطية.

وقد بدأ هذا بسلسلة من الإشارات ذات المعنى المزدوج والاستجابات البطيئة والفرص الضائعة من جانب الحزب الديمقراطي لتحديد مصدر هذه الهجمات غير المسبوقة والرد عليها. وكانت النتيجة حدوث أزمة كبرى للديمقراطيين ومؤامرة سياسية دامت أشهُراً، وخدمت مصالح الحزب الجمهوري ومرشحه دونالد ترامب.

ومما كشفته عمليات الاختراق ما يلي:

- قبل ثلاثة أيام من المؤتمر الوطني الديمقراطي، كشفت مؤسسة ويكيليكس ما يزيد على ٤٤ ألف رسالة بريد إلكتروني ظهر من خلال بعضها تحيز ديبي واسرمان شولتز (رئيسة اللجنة الوطنية الديمقراطية التي من المفترض أن تكون حيادية تجاه جميع المرشحين) الشديد لهيلاري كلينتون ضد منافسها عضو مجلس الشيوخ بيرني ساندرز. وانتهى الأمر بإجبار شولتز على الاستقالة بصورة مخزية؛ بعد أن تهاوت مصداقيتها.
- تم الكشف عن الميزانية اللازمة والخطة المتبعة في حملة اللجنة الوطنية الديمقراطية، ولم تكن الخطة سوى مسودة للحملة، وكانت بمنزلة كنز من المعلومات لحملة ترامب.
- تبادل جون بوديستا، رئيس حملة كلينتون، مراسلات مع رئيس الأركان رون كلين بشأن جو بايدن ظهرت من خلالها خيانة كلين لبايدن؛ من أجل الانضمام إلى حملة كلينتون.
- في رسالة إلكترونية إلى صديق، ادَّعى بوديستا أن هيلاري كلينتون لديها «غرائز سياسية بشعة».
- قيل إن كلينتون كانت تفكر، في حال انتخابها رئيساً، بالتدخل في سوريا بشكل سري.
- في حديث خاص، اقترحت كلينتون تقليص أسلحة الدفاع الأساسية.
- ظهر أيضاً أن كلينتون كانت تدعم مفهوم الحدود المفتوحة، وهو واحد من أهم القضايا السياسية المحلية التي كان لترامب حيالها رأي مخالف.
- قالت كلينتون: إنها «تخطط لبذر الثورة على ممارسات العصور الوسطى» التي تقوم بها الكنيسة الكاثوليكية؛ مع أن الكاثوليك يمثلون الكتلة الانتخابية الأكبر في الولايات المتحدة الأمريكية، كما أن جون كينيدي، الرئيس الكاثوليكي الوحيد في تاريخ الولايات المتحدة، كان عضواً في الحزب الديمقراطي.

- اعترفت كلينتون باتخاذها مواقف مختلفة على الصعيدين العام والخاص حيال قضايا بعينها؛ ما زاد في شكوك الناخبين في مصداقيتها.

ولم يكن هذا الكشف، أو غيره، سبب إحراج الديمقراطيين وحملة كلينتون فحسب؛ بل إنه أثار الكثير من الاضطراب والتشتت الداخلي في أثناء الحملة، كما أثَّر بشكل سلبي في سمعة أعضائها.

وكان هناك فريقان من الروس يعملان ضد الديمقراطيين، أحدهما يعمل نيابةً عن المخابرات العسكرية الروسية، والآخر نيابةً عن المخابرات المدنية. وقد أشار معظم التقارير إلى أن الفريقين لم يُنسِّقا أنشطتهما معاً. ومن المستحيل معرفة إذا كان عدم التنسيق هذا مُتعمَّداً أم لا.

وكان لعمليات القرصنة الروسية شركاء متواطئون وآخرون خدموها من غير قصد؛ فقد بدأت العملية كمحاولة بسيطة لجمع المعلومات عن الديمقراطيين. ومع اتساع نطاق المعلومات التي تمكنوا من الوصول إليها، قدَّم المخترقون الروس ما حصلوا عليه من معلومات إلى جوليان آسانــج. ومن الجدير بالذكر أن آسانــج الهارب من تهم جنائية في موطنه بالسويد، ويعيش حالياً في منفاه بسفارة الإكوادور في لندن، أنكر أنه تلقى، هو أو مجموعته، الوثائق من روسيا. أما المواقع الإلكترونية الأخرى، مثل DCLeaks.com فقد حصلت على معلومات أيضاً، وقامت بنشرها.

أصبحت المواقع التي نشرت المعلومات التي تم تسريبها مصادرَ للمؤسسات الإعلامية الكبرى بالولايات المتحدة الأمريكية، مثل: صحيفتي نيويورك تايمز، وواشنطن بوست، بالإضافة إلى وكالات الأخبار الأجنبية. وقد أظهر كثير من المؤسسات الإعلامية سوء الأداء وسوء الإدارة عندما عجزت عن التحقُّق ممَّن كان وراء هذا القدر الوافر من التسريبات التي استندت أهم أخبارها إليها، على الرغم من أن المسؤولين في الحزب الديمقراطي لم ينكروا مصداقية الوثائق المسربة.

وبمجرد نجاحهم في الوصول إلى الملفات التابعة للَّجنة الوطنية الديمقراطية، استهدف القراصنة الروس المراسلات الإلكترونية بين المسؤولين في حملة كلينتون، واكتشفوا أن مدير الحملة جون بوديستا – الذي كان يعمل بشكل مستقل بعيداً عن اللجنة الوطنية الديمقراطية – كان متراخياً حيال البروتوكولات الأمنية. ومع مرور الوقت استطاع

القراصنة الوصول إلى ما يقرب من ستين ألف رسالة إلكترونية قام بوديستا بإرسالها أو تَلَقِّيها.

## انتخابات في مهب الريح

كانت الانتخابات الأمريكية الأخيرة من أكثر الانتخابات إثارةً للخلافات والنزاعات في التاريخ الأمريكي، وكان أكثر ما أسهم في هذا السلسلةُ غيرُ المتناهية من التسريبات التي تم الحصول عليها إثر اختراق الحزب الديمقراطي والمراسلات الخاصة بحملة كلينتون. ومع رصد نتائج الانتخابات وظهور فوز دونالد ترامب؛ ظل سؤال واحد من دون إجابة، هو: هل أثَّرت عمليات القرصنة تلك في النتائج أم لا؟ لا توجد إجابة قاطعة عن هذا السؤال. ولا شك في أن ترامب والحزب الجمهوري استفادا من تلك التسريبات بشأن معارضيهم من الحزب الديمقراطي، ولكنْ، سيظل عدد الناخبين المتأثرين بالتسريبات غير معروف.

كما أن هناك كثيراً من العوامل المؤثرة الأخرى في أثناء الحملة الانتخابية، أدت بدورها إلى فوز ترامب، من ضمنها قدرته على الاستفادة من الإحباط الذي شعر به المواطنون الأمريكيون بسبب أداء الحكومة، والأخطاء الجسيمة التي ارتكبتها حملة كلينتون ومستشاروها. فعلى سبيل المثال، أخفقت كلينتون في الكثير من الولايات الرئيسية في الغرب الأوسط، وخسرت أصواتها الانتخابية لصالح ترامب. كما أن استقطاب ترامب المواطنين الأمريكيين قابله نفورُ شريحةٍ من الناخبين الأمريكيين من كلينتون؛ بما في ذلك النساء اللاتي افترضت كلينتون أنهن سيدعمنها. ولهذه الأسباب يستحيل استنتاج إذا كان الهدف الروسي هو التأثير في نتيجة الانتخابات. وفي السياق نفسه لا يوجد دليل على حدوث تلاعب في أيٍّ من أماكن الاقتراع بالولايات المتحدة الأمريكية.

وهذا لا يعني أن عمليات الاختراق الروسي لم تكن ذات أهمية؛ فالمخابرات الأمريكية كان لها رأي في هذا الشأن؛ فبعد الانتخابات في نوفمبر ٢٠١٦م بمدة وجيزة، أصدرت إدارة الأمن الوطني ومدير المخابرات الوطنية بياناً قصيراً مشتركاً قالا فيه: إنهما كانا «على ثقة» بأن الحكومة الروسية هي مصدر المعلومات التي تم تسريبها.

ولم يذكر التقرير اسم بوتين صراحةً، لكنه أثار قدراً من الشك حيال ما إذا كانت المخابرات تعتقد أن كبار المسؤولين في الحكومة الروسية سمحوا بتلك الهجمات.

وكانت هذه هي المرة الثانية التي تشير فيها الولايات المتحدة الأمريكية إلى تورط إحدى الحكومات الأجنبية في هجمات إلكترونية؛ أما المرة الأولى فكانت منذ عدة سنوات عندما ألمحت الولايات المتحدة إلى تورُّط كوريا الشمالية في هجمات إلكترونية على شركة سوني.

وعلى الرغم من الآراء القوية والموحدة لمنظمات الأمن القومي الأمريكية، فإن دونالد ترامب لم يكن مستعداً للاعتراف بأن روسيا هي مصدر عمليات الاختراق؛ بل قال: إن الاختراق لم يقع مطلقاً، ووصف تلك التهم بأنها «سخيفة». وقد يبدو هذا ردَّ فعل مقبولاً من ناحية؛ فاعتراف ترامب بعمليات الاختراق قد يشحذ همم أولئك الذين شككوا في فوزه، وأنه كان غير مشروع. وما زاد الشكوك في فوز ترامب أن بعض الآراء التي لم يتم توثيقها أو التحقُّق منها أشارت إلى أن مسؤولي حملة ترامب قد يكونون متواطئين في عمليات الاختراق التي قام بها الروس.

بعد أن عبَّر ترامب عن آرائه كان لا بد من إصدار بيان موجز ومنسق من قِبَلِ مدير المخابرات الوطنية جيمس كلابر، ومدير وكالة الاستخبارات العسكرية جون برينان، ومدير مكتب التحقيقات الفيدرالية جيمس كومي. وعلى مدار ساعتين كاملتين، وقبل أيام قليلة من مراسم أداء اليمين الدستورية، قام ثلاثتهم بمراجعة ما لديهم من أدلة، وتوصلوا - من دون أي تحفظات - إلى أن فلاديمير بوتين أصدر أوامره بشكل مباشر لتنفيذ عملية اختراق ضد الانتخابات الرئاسية الأمريكية. وجاء رد ترامب بأن هناك دولاً أخرى غير روسيا، مثل: الصين وإيران، تقوم بهجمات إلكترونية على الولايات المتحدة.

ولم تكن هيلاري كلينتون والحزب الديمقراطي هما وحدهما ضحايا عمليات الاختراق الروسية؛ فقد ظهرت أخبار تلك العمليات في عناوين عريضة في الصحف الوطنية والدولية، ولكنها لم تكن الوسيلة الوحيدة التي اتبعتها روسيا لإثارة القلاقل في انتخابات عام ٢٠١٦م؛ فوفقاً لتقرير نيويورك تايمز امتدت عمليات الاختراق الروسية ضد الديمقراطيين؛ لتشمل عدداً من السباقات التي يخوضها الديمقراطيون في أنحاء البلاد لشغل مقاعد في مجلس النواب الأمريكي[٧]، الذي تكمن أهميته في كونه مسؤولاً عن سنِّ التشريعات الخارجية والمحلية؛ بما في ذلك أنواع الحظر التي أحدثت ضرراً

(7) Eric Lipton and Scott Shane, "Democratic House Candidates Were Also Targets of Russian Hacking," *New York Times*, December 13, 2016.

جسيماً بالاقتصاد الروسي. فقد استهدفت عمليات الاختراق الروسية أجهزة عدد من مرشحي الحزب الديمقراطي لمجلس النواب، كما استهدفت سرقة آلاف الوثائق من لجنة الكونجرس الديمقراطية في واشنطن العاصمة، الموجودة في المبنى نفسه الذي تقع فيه اللجنة الوطنية الديمقراطية. وقد أظهرت التحقيقات احتمالية أن تكون عمليات الاختراق بدأت في مارس أو أبريل ٢٠١٦م، ولم يتم إدراك كنهها حتى أغسطس ٢٠١٦م. ومن أهم الميزات التي يتمتع بها عادة القائمون بأعمال الاختراق – وليس دائماً كما هو الحال هنا – أنه نادراً ما يتم الكشف عن أنشطتهم سريعاً.

وبمجرد أن حصل المخترقون الروس على الوثائق الداخلية للحزب الديمقراطي؛ قاموا باستخدام مواقع التواصل الاجتماعي للاتصال بأعداد من الصحفيين والمدوِّنين وتزويدهم بالمعلومات التي تم الحصول عليها، مثلما فعلوا عند استهدافهم حملة كلينتون. وقد شملت هذه المواد الإعلامية السياسات الداخلية للحزب بشأن الانتخابات في أنحاء البلاد كافةً. كما كشفت مجموعة المخترقين الروس المُسماة (Guccifer 2.0) تقييم اللجنة الوطنية الديمقراطية لمرشحيها في نيويورك، وبنسلفانيا، وأوهايو، وإلينوي، ونيومكسيكو، وكارولينا الشمالية، وفلوريدا؛ فتم – على سبيل المثال – تقييم مرشحة فلوريدا بأنها ضعيفة، ولم تستطع جمع التبرعات، وهو التقييم الذي حكم على حملتها بالفشل.

وقد جاء رد فعل المسؤولين بالحزب الديمقراطي غاضباً إزاء هذا التلاعب. وصرَّح كيلي وارد المدير التنفيذي لحملة اللجنة الديمقراطية بالكونجرس، بأن انتقاد المعارضين المحليين لمرشحي الحزب أمرٌ، ومحاولةَ إحدى الدول إثارة الاضطرابات في الانتخابات الأمريكية أمرٌ آخر تماماً. وأضاف وارد أن الحزب الديمقراطي كان ضحية للنوع الآخر من الهجوم. أما فيما يتعلق بحملة الانتخابات الرئاسية، فلا توجد سبيل لمعرفة مدى تأثير المعلومات التي تم تسريبها على أيٍّ من المرشحين لمجلس النواب في مختلف أنحاء البلاد، لكنْ، في الانتخابات البرلمانية لعام ٢٠١٦م استطاع الحزب الجمهوري تحقيق انتصارات كبيرة، وحافظ على غالبية المقاعد في مجلس النواب.

### عقوبات غير مجدية

من المثير للسخرية أن الهجمات الإلكترونية الروسية كان يتم شنُّها على مرشحي الحزب

الديمقراطي، وليس على مرشحي الحزب الجمهوري؛ فمنذ نهاية الحرب العالمية الثانية، كان الحزب الديمقراطي هو الطرف الذي يسعى إلى إيجاد علاقات جيدة مع روسيا. والرئيس الأمريكي الأسبق بيل كلينتون - على سبيل المثال - بذل جهوداً كبيرة لدعم تحوُّل روسيا إلى ديمقراطية ناشئة عقب انهيار الاتحاد السوفيتي عام ١٩٩١م، لكنها لم تتكلل بالنجاح. أما الحزب الجمهوري فقد اشتهر بصرامته فيما يتعلق بالسياسة الخارجية ومواجهة روسيا، إلا أنه في البيئة الجديدة للهجمات الإلكترونية يمكن للأصدقاء القُدامى أن يصبحوا أعداءً جُدداً.

كان باراك أوباما على عِلْمٍ بما يجري على مدار أشهُر؛ فقام - على غير عادته - بدراسة المشكلة بشكل مكثف. وعلى الرغم من حثِّ طاقم العمل الخاص به المستمر؛ إلا أنه لم يتخذ أي إجراء للانتقام مما جرى. ولا يمكن أن يُتوقَّع من هذا الضعف أن يردع تصرفات روسيا مُستقبلاً؛ فبعد أشهُر من السلبية في مواجهة هذه السلسلة غير المتناهية من عمليات الاختراق الروسية وحرب المعلومات؛ قرر أوباما أخيراً اتخاذ إجراء في الأيام الأخيرة من رئاسته؛ ففي أواخر ديسمبر ٢٠١٦م، قبل أسابيع من مغادرته منصبه، أصدر أوباما أوامره بطرد خمسة وثلاثين من الدبلوماسيين الروس وعائلاتهم من الولايات المتحدة الأمريكية. واقتصر الطرد على مَنْ كان وراء الأنشطة الروسية بواشنطن العاصمة، وكذلك سان فرانسيسكو، التي تمثل منطقة جذب مهمة؛ نظراً إلى قربها من وادي السيليكون.

كما أصدر أوباما أوامره بغلق المجمعات في ميريلاند ونيويورك، التي كانت تستخدمها الحكومة الروسية للقيام بأنشطة التجسُّس. وتم فرض الحظر على خدمة الأمن الاتحادية ومدير المخابرات الرئيسية وثلاث شركات روسية أُشيع عنها مساعدتها لروسيا في عمليات الاختراق؛ إلا أن إجراءات الحظر هذه لم تكن سوى إجراءات رمزية، ولم يكن لها أي تأثير فاعل. وعند عودة هؤلاء الدبلوماسيين إلى روسيا تم استقبالهم بحفاوة ودعوتهم إلى احتفالات الكريسماس ورأس السنة بالكرملين.

وقد وصف أوباما هذه الإجراءات بأنها ضرورية ولازمة. وكان يمكن لحكومة بوتين أن تنتقم بطرد عدد مماثل من الدبلوماسيين الأمريكيين من روسيا؛ إذ قامت بذلك كثيراً فيما سبق إبان الحرب الباردة. وقد طالب سيرجي لافروف وزير الخارجية الروسي بمثل هذا الإجراء، لَكِنَّ بوتين ردَّ بأنه لن ينتقم مما سمّاه «دبلوماسية المطبخ». وقد

ادَّعى ديمتري بيسكوف أن قرار أوباما غير قانوني. وعلى الرغم من الضجة التي أثارها القرار توقَّع خبراء مكافحة التجسُّس بالولايات المتحدة الأمريكية أن يكون لهذا الطرد تأثير قصير المدى على عمليات التجسُّس الروسية.

وحتى في الوقت الذي كانت فيه المنظمات الحكومية الروسية تُنَفِّذُ هجمات ذات دوافع سياسية صرفة على العملية الانتخابية الأمريكية، كان مجرمو الإنترنت الروس يقومون بشكل آخر من الهجمات الإلكترونية على أهداف أمريكية؛ فقد ورد في أحد التقارير الصادرة عن نيويورك تايمز عام ٢٠١٦م أن «شبكة تزييف إلكترونية ضخمة أنشأت حسابات لأكثر من نصف مليون مستخدم مزيف على الإنترنت و٢٥٠ ألف موقع إلكتروني مزيف لخداع المعلنين؛ لدفع مبالغ تصل إلى خمسة ملايين دولار في اليوم مقابل إعلانات فيديو لم يتم مشاهدتها مطلقاً»[٨].

وقد استطاع هؤلاء اللصوص فعل ذلك بانتحالهم شخصيات ما يزيد على ستة آلاف ناشر؛ حتى يتمكنوا من سرقة عائدات الإعلانات من المواقع الأخرى. وقد كان نجاحهم نتيجة «لأخطاء في نظام الإعلانات شملت عدم وجود وسيلة ثابتة وموثوق بها لتتبُّع الإعلانات وضمان عرضها على الجمهور المستهدف»[٩].

ومع إثبات هشاشة وسائل الإعلام الأمريكية الأكثر شهرةً وسهولةً للتعرض للاختراق؛ فقد أُشيع أن صحيفتي وول ستريت جورنال، ونيويورك تايمز، ومحطات فوكس، وسي بي إس الرياضية وقعت جميعها ضحية لعمليات الاحتيال على الإنترنت (لا توجد صلة معروفة بين هذه العملية والهجمات الإلكترونية الموجهة من الكرملين ضد رجال السياسة الأمريكيين). ويقول مايكل تيفاني أحد خبراء حماية الحاسوب: «يقدم أعداؤنا أشكالاً جديدة من الابتكار في عالم تزييف الإعلانات»[١٠].

ووفقاً لصحيفة نيويورك تايمز؛ يمكن تلخيص هذا التطور الفريد لعمليات الاحتيال وكيفية تنفيذها على النحو التالي:

---

(8) Vindu Goel, "Selling Ads on Fake Sites, Russian Ring Steals up to $5 Million Daily," *New York Times*, December 21, 2016, B1.

(9) Goel, "Selling Ads."

(10) Goel, "Selling Ads."

- يبدأ المحتالون بتسجيل عناوين رقمية مزيفة على الإنترنت تخضع لسيطرتهم بصفتهم أحد مقدمي خدمة الإنترنت المشهورين، مثل: Cox, AT&T, Comcast.
- يقوم المحتالون بعدئذٍ بربط العناوين بما يزيد على ٥٠٠ ألف من الحاسبات الآلية المُصمَّمة لمحاكاة الأشخاص الذين يقومون بتصفح الإنترنت. وتوجد بمتصفح الإنترنت التابع لهذا الحاسب مواقع جغرافية وهمية وتواريخ مزيفة لزيارات مواقع أخرى.
- يقوم المحتالون بعد ذلك بربط الحاسبات بشبكات إعلان آلية لمساحات إعلانية غير مباعة للآلاف من المواقع على الإنترنت؛ فعلى سبيل المثال يمكن للحاسب «زيارة» موقع مثل CNN.com، ثم تقوم الشبكات بعد ذلك سريعاً بشن حرب بعضها على بعض لعرض مقطع فيديو إعلاني لمنتج معين. وبدلاً من زيارة متصفح CNN الأصلي يتم توجيه المستخدم إلى موقع وهمي لا يستطيع أحد رؤيته.
- وأخيراً، يقوم النظام بإرسال بيانات مزيفة إلى شبكات الإعلان والمُعلنين؛ لإقناعهم بأن هناك مَنْ شاهد الإعلان بالفعل على الموقع الأصلي الذي يضم المحتوى.

وثمة قلق متنامٍ بين الخبراء في تقنية المعلومات حيال مدى خطر كون البنية التحتية الحيوية عُرضةً للهجمات الإلكترونية؛ فقد استخدم الروس هذا الأسلوب ضد أوكرانيا في أواخر ديسمبر ٢٠١٥م، عندما عطلوا شبكة الكهرباء الأوكرانية. وأكدت التقارير اللاحقة أن الشبكات الجوية الأوكرانية والسكك الحديد والتعدين كانت جزءاً من أهداف ذلك الهجوم.

استرعت هذه الهجمات انتباه وكالة استخبارات الدفاع الأمريكية (DIA). وفي بداية عام ٢٠١٦م أصدرت الوكالة تقريراً، قالت فيه: «بما أن برمجيات الأمن الإلكتروني تُصنَّع من قِبَلِ شركة روسية المنشأ، هي (كاسبر سكاي لاب)؛ فقد يؤدي هذا إلى أن تصبح البنية التحتية الحيوية في الولايات المتحدة الأمريكية أكثر عُرضةً للهجمات الإلكترونية الروسية»[١١]. ووفقاً لهذا التقرير؛ فإن «استخدام هذه البرمجيات من قِبَلِ المرافق الأمريكية، من شأنه أن يُنشئ نقاط ضعف داخل أنظمة الرقابة الصناعية الأمريكية،

(11) Bill Gertz, *iWar: War and Peace in the Information Age*, Threshold Editions (New York: Simon and Schuster, 2017), 178.

وتحديداً داخل فئة من وحدات التحكم تُسمَّى نظام التحكم الإشرافي وتحصيل البيانات (SCADA)»[١٢].

ولم يكن هذا مجرد خطر افتراضي؛ فقد أظهرت الإحصاءات التابعة لإدارة الأمن الوطني الأمريكية «صعوداً في نسبة الهجمات الإلكترونية على البنية التحتية الحيوية بين عامي ٢٠١٠م و٢٠١٥م بلغت سبعة أضعاف». كما أوضح التقرير الصادر عن وكالة استخبارات الدفاع أن بعض مرافق الكهرباء والنفط والغاز والمياه الأمريكية كانت تدرس شراء هذا البرنامج. وأنكر المتحدث باسم شركة (كاسبر سكاي لاب) هذه الادعاءات، بينما سعى لتكوين شراكات مع المقاولين الأمريكيين للفوز بفرص عمل في الولايات المتحدة. وإضافة إلى هذه المخاوف، أدلى مدير المخابرات الوطنية السابق جيمس كلابر بشهادته أمام اللجنة الدائمة للاستخبارات في مجلس النواب عام ٢٠١٦م، وقال فيها: إن روسيا تجري «مراقبة إلكترونية» لشبكة الكهرباء الأمريكية، وغيرها من الأهداف المختارة. وكان كلابر يشير إلى ممارسات المتخصصين في حرب المعلومات الروسية، واختراقهم الحاسب الآلي الخاص بسلسلة شركات أمريكية تعمل في مجال البنية التحتية؛ من أجل الوصول إلى شبكات التحكم الصناعي. وقال: إنه في ثلاثة مواقف منفصلة، على الأقل، تعرضت سلاسل مُورِّدي منتجات أنظمة التحكم الصناعي للخطر[١٣].

ومن المفارقات أن أحد أكثر المخاوف الملحة لدى خبراء الأمن بالولايات المتحدة الأمريكية، يتمثل في أن الروس ربما لا يقومون بشيء يُذكر، أو بأي شيء على الإطلاق مما اكتسبوه من معارف وقدرات؛ لوجود احتمال بعدم استغلال نقاط الضعف الأمريكية إلا إذا حدثت أزمة في العلاقات.

وتُعَدُّ الولايات المتحدة حالياً أكثر الدول الغربية المستهدفة من الهجمات الإلكترونية الروسية. وقد توصل تقرير المخابرات الأمريكية، الذي قام بوصف عمليات الاختراق الروسية والحرب المعلوماتية الروسية في الولايات المتحدة، إلى أن روسيا سعت للتأثير في الانتخابات في شتى أنحاء أوروبا. لكن هذا لم يلقَ اهتماماً واسعاً من وسائل الإعلام.

(12) Gertz, *iWar*.

(13) Gertz, *iWar*, 185.

وتُعَدُّ ألمانيا مثالاً جيداً على اهتمام روسيا بالتأثير في نتائج الانتخابات في الغرب؛ فألمانيا ستقوم بإجراء انتخابات برلمانية في سبتمبر ٢٠١٧م؛ لاختيار قادة وطنيين، وتقرير ما إذا كانت المستشارة أنجيلا ميركل ستستمر في منصبها فترة رابعة أم لا. وهذه الانتخابات هي الأخرى هدف لعمليات الاختراق الروسية منذ قضية (متاهة ضوء القمر)؛ فألمانيا تمتلك كمّاً كبيراً من التقنية ذات المستوى العالمي التي تهم روسيا. وفي أواخر عام ٢٠١٦م اعترف مسؤولون ألمان بأن الكثير من عناوين البريد الإلكتروني الخاصة بمسؤولين رفيعي المستوى في الدولة تعرضت للاختراق، وأن أصابع الاتهام تشير إلى روسيا.

ولا تزال هذه التقارير مستمرة في التداول، وتفيد بتنفيذ أنواع مختلفة من الدعاية وعمليات السيطرة. ويقول أحد المصادر: إن روساً أنشؤوا حسابات بنكية في سويسرا؛ لتمويل عمليات السيطرة هذه. وقد أبلغت الحكومة الألمانية البرلمان الألماني في أواخر ديسمبر ٢٠١٦م، أن شبكات الحاسب الآلي في ألمانيا تعرضت لعمليات اختراق مستمرة على مدار العام الماضي من قِبَلِ عدة أجهزة مخابرات أجنبية؛ بما في ذلك روسيا. وتوصل التقرير إلى احتمال وجود هجمات إلكترونية على حملة الانتخابات الاتحادية في ألمانيا. كما حدَّد التقرير نفسه روسيا مصدراً للهجمات التي تم شَنُّها في شهري مايو وأغسطس ٢٠١٦م على البرلمان الألماني والأحزاب السياسية الوطنية. وكانت أداة الاختراق التي استخدمتها روسيا ضد ألمانيا نوعاً من البرمجيات الخبيثة يُعرف بـ(APT 28).

كما كانت هناك عمليات أخرى تجري في فرنسا؛ حيث يتم انتخاب قادة قوميين جُدد، وكانت روسيا وراء الهجمات التي تم شنُّها في أبريل ٢٠١٥م على قناة الأخبار الفرنسية الشهيرة (Monde25). وقيل إن هذا الهجوم تم أيضاً باستخدام برنامج (APT 28). ومن المعروف أن مارين لوبان، المرشحة للرئاسة الفرنسية، من أكبر داعمي روسيا، وقد كُتب الكثير من المقالات لصالحها - جاء بعضها من مصادر مشبوهة - في وسائل الإعلام.

وفي الوقت نفسه تعرَّض إيمانويل ماكرون، أحد المرشحين للرئاسة الفرنسية، والمعروف بعدائه لروسيا، إلى سلسلة من الهجمات في وسائل الإعلام شملت اتهامات بكونه شاذّاً جنسياً. وبالطبع لا توجد أدلة على دعم الاتهامات ضد أيٍّ من المرشحين، ولكنَّ الحكم في نهاية الأمر هو للشعب الفرنسي الذي سيقرر إذا كانت هذه الادعاءات صحيحة أم كاذبة.

إن إثارة هذا الارتباك في أذهان الناخبين هي انتصارٌ للروس الذين سيقومون، بدورهم، بالتشكيك في نزاهة الانتخابات في كل من ألمانيا وفرنسا؛ فالتلاعب السياسي لا يؤثر في المُهاجم إلا بقدر ضئيل.

## الخاتمة

الدروس المُستفادة من الأنشطة الإلكترونية الروسية متنوعة ومهمة للغاية بالنسبة إلى الولايات المتحدة والديمقراطيات الغربية الأخرى. كما ستستفيد دول الشرق الأوسط، التي هي صديقة للغرب - بشكل مؤكد - من تلك الدروس أيضاً. وفوق ذلك كله، فإن روسيا خصم عنيد ينظر بريبة إلى علاقاته مع الغرب، ولاسيما الولايات المتحدة، ويقف تجاههم جميعاً على حدود صفرية.

وينطبق ذلك على جميع الأنشطة؛ سواء في أوقات السلم أم أوقات الحرب؛ إذ إن هذه المصطلحات تُستخدم في الغرب. وبالنسبة إلى بوتين ومَنْ حوله في (الكرملين)، فإن أي شيء يحقق مصالح روسيا أو يعرقل مصالح الولايات المتحدة أو الغرب هو أمر إيجابي. وكما يتضح من خلال الهجمات واسعة النطاق على هيلاري كلينتون؛ فإن هذا يشمل الجهود الرامية إلى تسوية أمور شخصية. وهذا ليس سوى جزء من جدول الأعمال الروسي الذي يهدف أساساً إلى تقويض الديمقراطيات والمؤسسات الغربية.

كما أن روسيا ترى نفسها في حالة تنافس مستمر مع الولايات المتحدة الأمريكية؛ فبوتين ضابط الاستخبارات السابق صرَّح، في أكثر من مناسبة، بأن انهيار الاتحاد السوفيتي كان أعظم كارثة شهدها القرن العشرون، كما استمر في تعامله وتفكيره كضابط استخبارات.

ومن هذا المنظور؛ فإن الحرب المعلوماتية التي تشمل: الهجمات الإلكترونية، والقصص المزيفة، وعمليات التأثير وبسط النفوذ، وأي أشكال أخرى من الدعاية، هي مجرد وسيلة لخدمة هدف سياسي أكبر، هو تقوية روسيا عن طريق إضعاف الولايات المتحدة الأمريكية وحلفائها.

وقد كانت الهجمات الإلكترونية السياسية الروسية، فضلاً عن الجرائم الإلكترونية الجنائية ضد الولايات المتحدة، ناجحةً للغاية. ولهذا السبب؛ فمن المؤكد أنها ستستمر.

كان نطاق هذه المجهودات مذهلاً؛ فإن إخفاق إدارة أوباما المتعمَّد - على مدار سنوات - شجَّع الروس على اتخاذ إجراءات سياسية من شأنها أن تُظهِر تصميم أمريكا على الاستجابة للاستفزازات الروسية؛ فالهجمات الإلكترونية الروسية هي شكل من أشكال الحرب. ومع أنها شكل يختلف تماماً عن الحروب في العصور القديمة أو حتى قبل بضعة عقود؛ إلا أنها لا تزال حرباً. وإلى أن تقبل الولايات المتحدة وأصدقاؤها وحلفاؤها هذا الواقع؛ فإنهم سيظلون مُعرَّضين بشدة للهجمات الإلكترونية في المستقبل.

لقد استفادت روسيا، إضافة إلى الصين، وإيران، وكوريا الشمالية، من واقع عدم وجود معايير متفق عليها لتنظيم أنشطة شبكات الاتصال والهجمات الإلكترونية. وكما هو الحال مع مجرمي الإنترنت والمنظمات الإرهابية التي تستخدم الهجمات الإلكترونية لخدمة أغراضها؛ فإن الحكومات المنبوذة بسبب نشاطها الضارّ في هذا المجال لا يطالها سوى قدر ضئيل من العقاب، أو لا يطالها شيء منه على الإطلاق.

وكما أكد كلٌّ من السيناتور جون ماكين وليندساي جراهام - عقب عملية الاختراق الأخيرة -؛ فإن طرد بعض الجواسيس والدبلوماسيين الروس من الولايات المتحدة الأمريكية «ما هو إلا ثمن قليل لهجوم روسيا الوقح على الديمقراطية الأمريكية»[١٤].

ومن الأسباب التي لا تجعل روسيا والدول الأخرى عُرضةً للمساءلة عن أنشطتها الإلكترونية عدم وجود رغبة دولية في فعل ذلك؛ فضحايا الأنشطة الإلكترونية لا يقتصرون على الولايات المتحدة وحلفائها فحسب؛ ففي الشرق الأوسط - على سبيل المثال - وقعت دول كبرى، مثل: المملكة العربية السعودية ضحيةً للحرب المعلوماتية. ومع أن كل دولة تسعى لحماية مصالحها القومية؛ إلا أن عدم رغبة المجتمع الدولي في تحريك هذه القضايا يجعل من الصعب على الدول الدفاع عن نفسها.

ومع أن الأمم المتحدة هي المنظمة التي يجب عليها معالجة هذه القضايا، إلا أنها دائماً ما تتعامل معها بمعايير مزدوجة، خصوصاً المتعلقة بدول، مثل: روسيا، والصين، وإيران.

لقد اتخذت الهجمات الإلكترونية - مؤخراً - بُعداً جديداً؛ ببثِّ الأخبار المزيفة؛ لتقويض الأفراد أو الحكومات؛ ما يُعَدُّ خروجاً على المحور الرئيسي للهجمات الإلكترونية، مثل:

(14) Sush Kreps and Debak Das, "Americans Are United on Retaliation against Russian Cyber Attacks," January 19, 2017 at www.washingtonpost.com.

الهجوم على هيلاري كلينتون واللجنة الوطنية الديمقراطية من قِبَلِ روسيا، الذي تم عن طريق تسريب رسائل البريد الإلكتروني المشروعة وغيرها من أشكال الاتصال الداخلي.

لقد ولجنا الآن عصراً يتم فيه خلط المعلومات الصحيحة – بغضِّ النظر عن كيفية جمعها ونشرها – بقصص وأخبار وهمية. وعلى سبيل المثال؛ تدَّعي إدارة ترامب أن شبكة سي إن إن الإعلامية الأمريكية العملاقة نشرت أخباراً مزيفة، زاعمةً أن لدى روسيا ملفاً من المعلومات عن الرئيس تساوم عليه.

وتزعم تقارير أخرى – نُشرت خلال الحملة الرئاسية الأمريكية – أن مساعدي ترامب اجتمعوا مع نظرائهم الروس أو ربما تواطؤوا معهم؛ لمساعدتهم في تقويض حملة كلينتون. هذه هي المزاعم التي تواجهها إدارة ترامب الجديدة في بداية ردِّها على التهديدات الإلكترونية. وقد أسند ترامب إلى صديقه القديم رئيس بلدية نيويورك السابق رودي جولياني مهمة وضع الاستراتيجية الإلكترونية للإدارة الأمريكية الجديدة، التي ستكون حقّاً مهمة كبرى.

## الكاتب في سطور

د. جاك كارافيللي: تقلَّد مناصب تحليلية وإدارية في كلٍّ من: وكالة الاستخبارات المركزية الأمريكية، ومجلس الأمن القومي الأمريكي، وكان المستشار الأول للرئيس بيل كلينتون في القضايا المتعلقة بمنع الانتشار النووي في روسيا والشرق الأوسط، كما عمل مع وزارة الطاقة الأمريكية؛ حيث أشرف على عدد من برامج الحدِّ من خطر انتشار السلاح النووي.

ومنذ أن ترك وظائفه الحكومية، قام كارافيللي بتأليف أربعة كتب، وأدلى بتصريحات حول قضايا الأمن القومي في الولايات المتحدة وخارجها. وفي عام ٢٠١٥م ترأس مؤتمراً عن الأنشطة الإلكترونية في لوغانو بسويسرا، ومن المتوقع أن يترأس مؤتمراً دولياً آخر عن الأنشطة الإلكترونية في عام ٢٠١٧م. كتب كارافيللي عن القضايا الإلكترونية؛ بما في ذلك مقالاته في المجلة البريطانية الدورية Cyber Security Review، وكثيراً ما يشارك في برامج إذاعية وتلفزيونية بالولايات المتحدة الأمريكية. وفي عام ٢٠١٦م أصبح رئيساً لمؤسسة نيوجن جلوبال، وهي شركة استشارات دولية تعمل في مجال التكنولوجيا.

## الكاتب المُشارك

سيباستيان ماير: حصل على البكالوريوس في العلوم السياسية والقانونية (٢٠١٣م) من جامعة ميونيخ، وبكالوريوس آخر من كلية العلوم السياسية في باريس. كما حصل على الماجستير في علوم الاستخبارات والأمن الدولي (٢٠١٤م) من قسم دراسات الحرب بكلية كينغز في جامعة لندن.

في عام ٢٠١٥م انضم إلى فريق العمل بمركز الملك فيصل للبحوث والدراسات الإسلامية باحثاً في وحدة الفكر السياسي المعاصر. وعمل، قبل انضمامه إلى المركز، متدرباً في السفارة الكندية بألمانيا، ومكتب الاتصال الألماني السعودي للشؤون الاقتصادية بالرياض. وتنصبُّ دراساته على الصراع السوري، وتورُّط روسيا وإيران وحزب الله في سوريا. ويقدم منذ عام ٢٠١٦م استشارات استراتيـجية للحكومات والشركات العالمية.

## مركز الملك فيصل للبحوث والدراسات الإسلامية

تأسّس المركز سنة ١٤٠٣هـ/ ١٩٨٣م لمواصلة الرسالة النبيلة للملك فيصل بن عبدالعزيز -رحمه الله- في نشر العلم والمعرفة بين المملكة وبقية دول العالم. ويعدُّ المركز منصةَ بحثٍ تجمع بين الباحثين والمؤسسات لحفظ العمل العلمي ونشره وإنتاجه، وإثراء الحياة الثقافية والفكرية في المملكة العربية السعودية، والعمل بوابةً وجسراً للتواصل شرقاً وغرباً. ويرأس مجلس إدارة المركز صاحب السمو الملكي الأمير تركي الفيصل بن عبدالعزيز، وأمينه العام هو الدكتور سعود بن صالح السرحان.

ويقدّم المركز تحليلات متعمّقة حول القضايا السياسية المعاصرة، والدراسات السعودية، ودراسات شمال إفريقيا والمغرب العربي، والدراسات الإيرانية والآسيوية، ودراسات الطاقة، ودراسات اللغة العربية والحداثة. ويتعاون المركز مع مؤسسات البحث العلمي المرموقة في مختلف دول العالم، ويضمّ نخبةً من الباحثين المتميّزين، وله علاقة واسعة مع عددٍ من الباحثين المتخصّصين في مختلف المجالات البحثية. ويحتضن المركز مكتبة الملك فيصل، ومجموعة مخطوطات نادرة، ومتحفاً إسلامياً، وقاعة الملك فيصل التذكارية، وبرنامج الباحثين الزائرين. ويهدف المركز إلى توسيع نطاق المؤلَّفات والبحوث الحالية لتقديمها إلى صدارة المناقشات والاهتمامات العلمية، متّبعاً مساهمة المجتمعات الإسلامية في العلوم الإنسانية والاجتماعية والفنون والآداب قديماً وحديثاً.

مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

P.O.Box 51049 Riyadh 11543 **Kingdom of Saudi Arabia**
Tel: (+966 11) 4652255 Ext: 8692 Fax: (+966 11) 4577611
**E-mail: research@kfcris.com**