**البيانات الضخمة في الاستخبارات العسكرية**

[**العدد 100 - نيسان 2017**](https://www.lebarmy.gov.lb/ar/content/100-d)

**البيانات الضخمة في الاستخبارات العسكرية**   
إعداد: د. يحيى طاهر   
 أستاذ وباحث في جامعة فرساي - باريس، وفي كلية العلوم في الجامعة اللبنانية

**المقدّمة**

يولّد تزايد كمية البيانات، وتنوّعها، وسرعتها مفهوم البيانات الضخمة الذي يندرج في قطاعات عدّة ومنها المجال العسكري. وتؤدي أدوات التكنولوجيا الحديثة ومنها إنترنت الأشياء "Internet of Things-IoT" إلى تغيير جذري في أنظمة المعلومات العسكرية. في السنوات الأخيرة، تمّ تصنيع العديد من الأشياء الذكية ومنها الأسلحة التي أسهمت بتغيير المشهد العسكري التقليدي. من جهةٍ أخرى، أصبحت مصادر معلومات أخرى مثل المصادر المفتوحة، أحد الأركان المهمة في عملية صنع القرار كونها تشكّل أحد أُسس عمل الاستخبارات العسكرية، بسبب استخدام شبكات المتطرّفين لها في مختلف أرجاء العالم. وبالتالي، إذا ما استطعنا التعامل معها مجتمعة بالكفاءة المطلوبة، بالإضافة الى المصادر العديدة الأخرى والتي يمكن أن توفّر كمِّا هائلًا من المعلومات، وذلك من خلال تحليلها بطريقة أعمق وأوسع ومن خلال استخراج الأنماط والمؤشرات والدلائل والتنبؤات للعمل بدقّة وبفعالية أكبر في مواجهة الارهابيين. في المقابل، لا تُعتبر عملية تحليل البيانات الضخمة سهلة، إذ تتوافر الكثير من التحديات المتعلقة بحجم هذه البيانات وسرعتها وتنوعّها.

تتوافر بعض الحلول المرتبطة بعملية تحليل البيانات الضخمة مثل "Modus Operandi", غير أنّ هذه الحلول، ما زالت تفتقر، إلى القدرة على توفير تحليل للبيانات في الوقت الفعلي، أو على تحليل البيانات برؤية تنبؤية للمستقبل. تركّز هذه الدراسة على الجوانب المختلفة للبيانات الضخمة، ودورها في الشؤون العسكرية، وتبيّن مختلف أنواع تكنولوجيا البيانات الضخمة والتحديات التي تواجهها، بالإضافة إلى تحديد المجالات المختلفة التي يمكن فيها استخدام البيانات الضخمة في الاستخبارات العسكرية. وتقترح الدراسة هندسة نظام لمعالجة النواقص التي تظهرها الحلول الحالية بغية تحليل البيانات الضخمة في الوقت الآني أو الفعلي.

**1- نشوء البيانات الضخمة**

يستخدم الأشخاص، في عصرنا الرقمي، آلاف الأجهزة في حياتهم العملية واليومية. فوفق "chui et al" [٩]، سيضم العالم، بحلول العام 2020، أكثر من 50 بليون جهاز متّصل بسبعة بلايين شخص، بالإضافة، إلى تطبيقات عدّة مثل وسائل التواصل الاجتماعي، المدوّنات وغيرها المتوافرة على الويب، والتي يستخدمها بلايين المستخدمين. كذلك، توفّر زيادة استخدام أنواع عدة من الأجهزة والتطبيقات كمية هائلة من البيانات الضخمة. فعلى سبيل المثال، يولّد تويتر، لوحده، سبعة تيرابايت (١٢١٠) (وحدة قياس لسعة التخزين في الحاسوب) يوميًا، ويستخدم بليون شخص موقع الفايسبوك يوميًا، ويتم، في الدقيقة الواحدة، إرسال نحو 31.25 مليون رسالة، ومشاهدة 2.77 مليون فيديو، وتحميل 300 ساعة فيديو على موقع "youtube". من جهةٍ أخرى، تقدّر مؤسسة البيانات الدولية (IDC-International Data Corporation) أنّ قطاع الأعمال على الإنترنت سيسجل 450 بليون عملية تجارية يوميًا بحلول العام 2020 [١][٣].

يسمح موقع "فايسبوك" بتخزين، وتحليل والوصول إلى أكثر من ثلاثين بيتابايت (1510) من البيانات العائدة للمستخدمين [٣]، وتوفّر أكثر من 300 مليون مدوّنة الكثير من البيانات [٢٥]. تجمع "المنظمة الأوروبية للأبحاث النووية–CERN" أكثر من 300 تيرابايت من البيانات بواسطة مصادم الهدرونات الكبير (Large Hadron Collider) [٢]. ويتضاعف حجم البيانات في الفضاء الرقمي، وفق IDC [٣]، كلّ سنتين. وسيبلغ حجم المعطيات التي سيولّدها الأفراد وينسخونها سنويًا بحلول العام 2020، 44 زيتابايت (2110) أو تريليون جيجابايت.

يؤدي هذا النمو غير المسبوق للبيانات إلى ظهور طوفان من البيانات أو ما يعرف "تسونامي البيانات"، ما يجعل من تحليل البيانات وإدارتها تحديًا جادًا، لا يأخذ بعين الإعتبار حجم البيانات فحسب، بل تنوّعها (من نصوص، صور، فيديو، وتسجيلات صوتية)، وسرعتها (سرعة حركة البيانات بين مختلف المراكز). تؤسّس هذه المعايير الثلاثة (الحجم، التنوع، والسرعة) لما يشكّل أبرز الإختراقات العلمية لهذا العقد "البيانات الضخمة- Big data".

**أ- تعريف البيانات الضخمة**

صاغ جون ماشي، في العام 1990، مصطلح "البيانات الضخمة". يعرّف غارتر [٥] البيانات الضخمة بمعلومات حجمها كبير، سرعتها عالية ومتنوّعة جدًا تستوجب آليات مبتكرة، فعّالة مقارنة بالكلفة لإدارتها ما يساعد على أخذ القرار، وعلى الإستبصار (insight)، وعلى عملية الأتمتة (automation). يركز ماكينسي [٤٠] على حجم البيانات الذي يتجاوز قدرة آليات البرمجيات النموذجية على الرصد، والتخزين، والإدارة والتحليل. غير أنّ التعريف الشامل يكمن في أنّ هذه البيانات الديناميكية، والكبيرة، والمتنوّعة التي يولّدها الأفراد، والآليات والآلات تستوجب أدوات تكنولوجية مبتكرة، ومتطوّرة لجمعها ولتحليلها بهدف توفير استبصار عملي مرتبط بالمستهلكين، وبالمنافع، وبالمخاطر، وبالأداء، وبالإنتاجية [٣٠]. ويلحظ مؤلفون آخرون أنّ البيانات الضخمة هي عبارة عن بيانات حجمها كبير، متنوّعة، تتولّد بسرعة عالية بنمط غير مؤكد لا يناسب تركيبة البيانات التقليدية، وتستوجب نظامًا معقدًا من البيانات مع منصّة حاسوبية "computing platform" وقدرات تحليلية [١٨]. تلحظ هذه التعريفات شقّين للبيانات الضخمة: الخصائص والقيمة .

توفّر البيانات الضخمة فرصًا كبيرة لقطاعات واسعة ومختلفة مثل المصارف وقطاع الأموال، التعليم، القطاع الصحي، الاتصالات، الخدمات العامة، والتأمين، وتشكّل مجالًا مهمًا للعلوم والابتكار. فعلى سبيل المثال، تندرج البيانات الضخمة في التجارب العلمية للحصول على نتائج أفضل، وفي البحوث في مجال العلوم الطبيعية، وفي الزراعة، وصناعات الغاز والبترول. ويلحظ باحثون آخرون، في الآونة الأخيرة، أهمية البيانات الضخمة في العمليات العسكرية وخصوصًا في مجال الذكاء العسكري أو الاستخبارات العسكرية، إذ إنّ هناك مجالات عدة يمكن فيها للبيانات الضخمة أن تعزّز الذكاء العسكري.

**ب- خصائص البيانات الضخمة**

ترتكز خصائص البيانات الضخمة على أربعة معايير: الحجم، التنوّع، السرعة، والدقة [١٤][٤١].

• الحجم: حجم البيانات وكميتها. يتراوح حجم البيانات بين تيرابايت وبيتابايت.

• التنوّع: تتوافر أنواع عدّة من البيانات والمصادر. وتتنوّع إدارة البيانات المعقدة بين المنظمة، شبه المنظمة وغير المنظمة.

• السرعة: سرعة توليد البيانات. فعلى عكس المقاربة الكلاسيكية، يتم توليد البيانات، اليوم، بوتيرة دائمة.

• الدقّة: يحال بالدقّة إلى الموثوقية المرتبطة ببعض أنواع البيانات. وبغية ضمان موثوقية البيانات، يجب طرح بعض الأسئلة المهمة: ما هو مصدر هذه البيانات؟ هل تعود هذه البيانات إلى مصدر موثوق؟ هل هي دقيقة؟

يضاف إلى هذه المعايير خصائص أخرى مثل:

• التبدّل: أو البيانات التي يتبدّل معناها بشكل دائم.

• القيمة: أو أهميّة وفائدة البيانات بالنسبة للشخص الذي يستهلكها.

• الكُمون: أو الوقت الضائع بين المعلومة والحدث المرتبط بها.

• الخصوبة: أو سرعة انتشار البيانات.

• التطاير: أو الفترة الزمنية لتوافر البيانات للمستخدم.

• القابلية: أو قابلية النجاح تضمنها نتائج تحليل البيانات.

تشكّل هذه الخصائص ركائز البيانات الضخمة، وعلى الأدوات التكنولوجية أن يكون لها القدرة على التعامل مع هذه الخصائص. تحتاج هذه الخصائص إلى طرق، وأدوات ونماذج تحليلية، وخوارزميات (algorithms) فعّالة يمكن استخدامها بطريقة سلسة في تطبيقات البيانات الضخمة.

**ج- مصادر البيانات**

تعتبر مصادر البيانات، اليوم، وفيرة ومتنوّعة، وهي تنقسم إلى نوعين: المصادر المرتبطة بالآلات، والمصادر المرتبطة بالأشخاص. يشكّل إنترنت الأشياء (Internet of Things-IoT) ونُظم معلومات المؤسسات مفاتيح المصادر المرتبطة بالآلات [٤٤]. يقصد بإنترنت الأشياء شبكة الروابط بين مختلف الأجهزة المتعلقة بالذكاء الإصطناعي مثل البيوت الذكية، المدن الذكية، التسوق الذكي، والصناعة الذكية. يعزّز إنترنت الأشياء ربط الأشياء بالأنظمة ما يؤدي إلى توزيع أكبر للأجهزة المرتبطة بأجهزة أخرى أو بالإنسان [٤٤]. يتم استخدام إنترنت الأشياء، اليوم، في المجال العسكري وخصوصًا في الأجهزة العسكرية الذكية وفي الأسلحة. تركّز التكنولوجيات العسكرية المرتبطة بإنترنت الأشياء على آليات القيادة والسيطرة والمراقبة والتواصل، الحواسيب، الذكاء، الإستطلاع (C4ISR)، ونظام السيطرة على الحرائق بالإضافة إلى توافر تطبيقات مهمّة في مجال إنترنت الأشياء, تتضمن أجهزة استشعار متطوّرة ونظام اتصالات بالأقمار الصناعية [٢١]. يساعد نظام إنترنت الأشياء الأجهزة العسكرية على توليد بيانات ضخمة.

سينتج نظام الأتمتة الصناعي (Industrial Automation Systems)، الذي يتم استخدامه في مجالات عدة ومنها: الدفاع، اللوجستية، الغاز، البترول، المصارف، الاتصالات، الصحّة والخدمات العامة، حجمًا كبيرًا من البيانات الضخمة. فعلى سبيل المثال، يولّد نظام الرسائل العسكرية وأدوات الحرب الإلكترونية كميّة ضخمة من البيانات، بالإضافة إلى أنّ مئات من برمجيات النظم (System Software) تولّد البيانات. يُسهم بروز الـ"Web 2.0" [٦] بإعطاء مساحة أكبر من الديمقراطية للمستخدمين في إنتاج موادهم ونشرها، فلم يعد، بالتالي، المستخدمون مستهلكين للبيانات فحسب، بل إنّهم ينتجون البيانات بمعدل غير مسبوق. يستخدم الأفراد أنواعًا عدّة من وسائل التواصل الاجتماعي، ومنها: Facebook, linkedIN, Myspace , و+Google. ويستخدم الأفراد الإيميل وسكايب، وواتساب، وفايبر، والمدوّنات الصغيرة لتبادل النصوص، والرسائل الصوتية والفيديو ما يولد كمية ضخمة من البيانات.

من جهةٍ أخرى، تربط الشبكة العالمية بلايين العقد (Nodes-الكود البرمجي الذي يستخدم لتخزين البيانات)، ما يؤدي إلى توليد سجلات البيانات بشكلٍ مستمر. توّلد التجارب العلمية بيانات ضخمة. فعلى سبيل المثال، توفّر التجارب التي تجري في مصادم الهدرونات الكبير أو في فكّ شيفرة الجينوم البشري، الكثير من البيانات مع توافر مئات أو آلاف مصادر أخرى للبيانات.

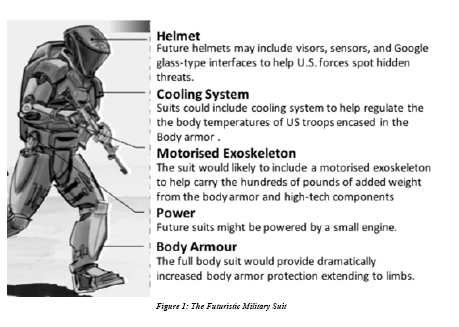
**2. المجال العسكري في عصر المعلومات**

يشير القائد العسكري وحاكم فرنسا نابليون بوناربت (1761-1821)، إلى أنّ الحرب تعتمد على المعلومات بنسبة تسعين في المئة. وعلى الرغم من أنّ بونابرت، الذي اشتهر بالحروب التي خاضها، لم يعش في عصر المعلومات، غير أنّه شدّد على أهمية المعلومات في التقدّم العسكري. واستمر الاهتمام بالمعلومات في هذا المجال فعلى سبيل المثال، كان لآلة "Enigma" التي ساعدت على فك الأسرار الألمانية، دور مهم في انتصار قوات التحالف في الحرب العالمية الثانية مع توافر أمثلة أخرى عدّة في شأن أهمية دور استخدام المعلومات في المجال العسكري. في السنوات الأخيرة، تمّ إدراج مفهوم حرب المعلومات (أو استخدام المعلومات وإدارتها للحصول على ميزة تنافسية على العدو) بغية جمع المعلومات التكتيكية عن الأعداء.

**أ- النظام العسكري المتّصل**

يتبدّل الواقع العسكري جذريّا في العصر الرقمي ما يشكّل ثورة في الحروب الحديثة. فيتزايد استخدام إنترنت الأشياء بوتيرة سريعة، مع ظهور وعود بتعزيز قدرات وفرص نجاة المحاربين، في ظل انخفاض الكلفة وتزايد الفعالية [١٦]. في الآونة الحديثة، صمّمت القوات المسلحة الأميركية، كما يظهر رسم 1، بزّة حديدية مرتبطة بتكنولوجيا إنترنت الأشياء، تشكّل الخوذة فيها جهاز استشعار أو مستشعر(Sensor). تسمح أجهزة الإستشعار الموجودة على الخوذة للجندي بأن يتّصل بأجهزة عدّة، وبأن يوفّر بيانات متعددة ومن بينها مجموعة من الصور.

يـضـع مـشــروع "DARPA" تـصـمـيـمًا لـمـركـبـة عـسـكرية ذكـيـة (XC2V FlypMode Military Assault Vehicle) مجهّزة بعدّة أنواع من أجهزة الإستشعار أو المجسّات التي يمكن لها أن تلتقط المعلومة في الوقت الفعلي، وأن تنقلها إلى موقع آخر مثل "Centralized Container" أو "Data Lake" [٢٤].



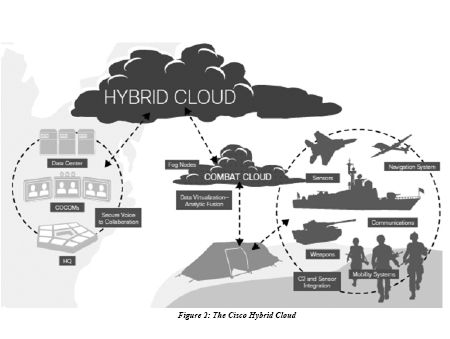
تشكّل الطائرة بلا طيار (drone) مثالًا لتكنولوجيا إنترنت الأشياء، ولتقدم التكنولوجيا العسكرية في العصر الحديث. وتتوافر أنواع عدة من الطائرات: منها ما يستخدم لجمع البيانات بواسطة "نظام التموضع العالمي-GPS" و الكاميرات التي تلتقط وترسل صورًا عن المواقع والأشياء [٣٨].  
يشكّل النظام الذي يتمتّع بشبكة اتصال كبيرة بين الأشياء أداة مهمّة لتوليد شبكة المعلومات في المجال العسكري, إذ يساعد هذا النظام على تشبيك أدوات عسكرية عدّة (ومنها: الرادار، الطائرات، الغوّاصات) وعلى جمع المعلومات وتبادلها بوتيرة أسرع وعلى تحليلها بكفاءة وفعاليّة. وبالإضافة، يعزّز إنترنت الأشياء النظام العسكري في ساحات المعارك من خلال تبادل المعلومات، وتحديد مواقع العدو على أرض المعركة وغيرها.

**ب- البنى التحتية لإنترنت الأشياء في المجالات العسكرية**

تحتاج الأدوات التكنولوجية المتعلّقة بأجهزة الإستشعار إلى بنى تحتيّة متطوّرة لإدارة تدفّق المعلومات ومراقبتها بأسلوب آمن، ولضمان ربط الأجهزة باستمرار من دون انقطاع في الاتصال، ولتحليل البيانات بفعالية بالوقت الفعلي أو على دفعات. يقترح نظام "Downing" [١٢] بنى تحتية مرتكزة على نظام الحوسبة السحابية (Cloud Computing) للعمليات المركزية. تساعد هذه البنى التحتية المتطوّرة على إدراج البيانات من مصادر عالمية متعدّدة في الوقت الفعلي لاتخاذ القرار.

توفّر "ميكروسوفت" بنى تحتية مرتكزة على نظام "السحابة" تعرف بـ "Microsoft Azure IoT Suite" [٢٢], تسمح للمؤسسات العسكرية بالإستفادة من المنصات بدرجة عالية وبطريقة فعّالة من حيث الكلفة من دون المساومة أو المخاطرة بعامل الأمن. يسمح النظام للعسكريين بإدراج الكثير من العتاد في أنظمتهم القائمة. بالإضافة إلى ذلك، يمكن لمنصة "C4ISR" إدراج البيانات المبنية والحلول في "Microsoft Azure Government Cloud" والمحافظة على هذه البيانات مع الإستفادة من كلفة بيئة سحابية آمنة ومنافعها [٢٢].

قامت "Cisco" بتطوير بنية تحتية مرتبطة بـ "IoT" للعسكر وتعتمد على "الحوسبة السحابية الهجينة (Hybrid Cloud)" [١٩]، كما يظهر رسم2. تدمج السحابة الهجينة بين السحابة العامة والخاصة. تظهر السحابة العامة تبادلًا للمصادر من عدّة زبائن بطريقة آمنة، بينما تُخصّص السحابة الخاصة من شبكة ومعدات لزبون واحد.



**3- البيانات الضخمة في المجال العسكري**

في السنوات القليلة الماضية، تنامت كميّة البيانات بشكل جذري في المجال العسكري من خلال استخدام نظام الأتمتة وإنترنت الأشياء. وأسهمت مجالات محاربة الإرهاب وأمن الشبكات بنمو البيانات المرتبطة بالمجال العسكري التي تولّدها، أيضًا، الكثير من العمليات العسكرية. فعلى سبيل المثال، تجمع طائرة واحدة من دون طيار "MQ-9 Reaper Drone"، التي تستخدم في مهمّات تجسّس، بيانات يوازي حجمها سعة 20 حاسوب محمول [٢٣]. وتحمل هذه الطائرات آلات لتسجيل فيديو في كلّ ثانية [٢٦].

يلتقط نظام المراقبة "The US ARGUS Ground" أكثر من 40 جيجابايت (910) من المعلومات في الثانية الواحدة [٢٣]. وتوفّر الأقمار الصناعية للتجسس بيانات جغرافية [٣١]. فيؤدي، بالتالي، نموّ البيانات بشكل غير مبني إلى أن يقتحم المجال العسكري عصر البيانات الضخمة.  
تؤثّر البيانات الضخمة ودورها في تعزيز الأمن العالمي, على عمل شركات الدفاع التي تتنافس في السوق. فأصبح من المهم أن يستثمر المسؤولون في المجال العسكري البيانات الضخمة بشكلٍ فعّال [٣١]. فتتركّز الوسيلة الأكثر فعالية في التعامل مع البيانات الضخمة على استخراج الدّلالات المعبّرة والمهمة في شأن الأمن القومي للمواطنين، وفي شأن حياة العسكريين في ساحات القتال [٣٦].

**أ- تعزيز نمو الذكاء الاستخباراتي**

تؤمّن البيانات الضخمة فرصًا جديدة لمفهوم الذكاء المجتمعي، وتعزّز نموّ الذكاء العسكري أو الاستخباراتي [١٥]. وتكمن الوعود الأعظم التي توفّرها البيانات الضخمة في القدرة على تعزيز دمج المعلومات وتنظيمها المرتبطة بمصادر عدّة ومنها: إنترنت الأشياء ووسائل التواصل الاجتماعي. تشكّل البيانات المرتبطة بمصادر خارجية عاملًا مهمًا في المجال العسكري، إذ تعتبر البيانات الركيزة الأساسية للتحليل العسكري أي الذكاء العسكري، ولنموّ فرص إنتاج المعارف الفعّالة.

ترتبط البيانات الضخمة بمجموعة من الآليات التكنولوجية الجديدة المتعلّقة بجمع البيانات، ونقلها، وتخزينها، وتنظيمها. توفّر هذه الأدوات التكنولوجية لمصادر التحليل إمكانية الوصول إلى البيانات بمزيد من الأتمتة والإنتاجية، ما يسمح، بذلك، بالتركيز على المشاكل الصعبة والتي لها الأولوية. وتسمح هذه الأدوات، وبشكل خاص، للمسؤولين في المجال العسكري بإدراج وسائل التواصل الاجتماعي في آليات التحليل للحصول على أجوبة للتساؤلات (لماذا، متى، ماذا، أين، من وكيف)، بالإضافة إلى أنّه يمكن تطبيق هذه التكنولوجيا الجديدة بشكل فعّال على مشكلات مرتبطة بالذكاء الدفاعي ومن ضمنها تحليل الشبكة الاجتماعية، برمجة أنظمة الأسلحة، تحليل الذكاء العسكري التكتيكي، أو إنذار لمشاكل عسكرية غير مألوفة، أو تحليل البنى مثل الإنتاج المرتبط بالأشياء، أو الذكاء المرتبط بالأنشطة. وبالتالي، لا تُعزّز هذه الإمكانيات القدرة على تنفيذ مهمات مرتبطة بالذكاء التقليدي، بل تنتج أنواعًا جديدة ومكثّفة لتحليل البيانات[٤٣].

ويعد العمل على البيانات الضخمة بتعزيز القدرة على فهم الشؤون المتعلقة بالذكاء التقليدي بطريقة أعمق، وبتحليل البيانات الضخمة، وتصوّرها، ودمجها، وتطوير الأدوات في شأن استخدامها لتعزيز البيانات الذكية وانتشارها بين العسكريين ووكالات الإستخبارات [١٠].

**ب- الأمن القومي**

يقترح هارديس [١٣] استخدامات عدّة للبيانات الضخمة في مجال الأمن القومي، مثل تحليل الأفراد من خلال شبكات التواصل الاجتماعي. فعلى سبيل المثال، تتضمّن النقاشات في مواضيع حسّاسة ودقيقة معلومات عن سلوكيات الأشخاص وبالتالي تحمل قيمة كبيرة. ويمكن التحليل والكشف عن أشخاص لديهم عدّة "بروفايلات" على شبكات التواصل (فيسبوك، تويتر، لينكد إن)، أو عن مجموعات نشطة على التواصل الاجتماعي. يشكّل تحليل شبكات التواصل أداةً فعّالة لمحاربة الإرهاب من خلال تحديد الشبكات الداعمة ومواقع الداعمين وتحليل البيانات. ويعتبر سبر البيانات (Information Mining) مثالًا آخر مهمًا على استخدام البيانات في مجال الأمن القومي. فيمكن جمع المعلومات في شأن شخص ما من مصادر متعدّدة، ثمّ ربطها وتحليلها بالوقت الفعلي لإستخراج الدلالات المهمة في شأن الأمن القومي ما يؤمّن تقدمًا على الأعداء، خصوصًا، في ساحة المعركة [١٣]. فعلى سبيل المثال، تساعد تيارات البيانات التي توفّرها أجهزة الإستشعار أو المجسات ومنها المرتبطة بالطائرات، الهليكوبتر، البدلات العسكرية، والطائرات بلا طيار، على إجراء تحليل معقّد ما يسمح بقيادة المعركة بكفاءة أكبر.

**ج- تحليل سلوكيات العسكريين**

يذكر سوكل [٢٧] أنّ مكتب الدفاع لحظ في العام 2008، تزايد الميول الإنتحارية بين العسكريين بنسب مقلقة. سجّلت وفيات الإنتحار في "الولايات المتحدة الأميركية"، في هذا العام، وفق مركز مكافحة الأمراض والوقاية منها (CDC)، معدّل 11.9 وفاة لكل 100 ألف شخص. بينما تبلغ نسبة الإنتحار في صفوف الجيش الأميركي 20.2 وفاة لكل 100 ألف شخص، أي ضعف المعدّل مقارنة مع المدنيين ما جعل إدارة القوات المسلحة تدرك أنّه يجب اتخاذ إجراءات سريعة وحاسمة. فأظهرت إدارة الجيش رغبة في البحث عن العوامل التي تدفع بالجنود إلى الإنتحار وتحديد المخاطر. وجد صنّاع القرار أنّ البيانات الضخمة يمكن لها أن تضطلع بدور حقيقي في تحديد الأنماط السلوكية للجنود. فقامت إدارة الجيش بجمع الكثير من البيانات المتعلقة بالجنود بغية تحديد العناصر الأكثر عرضة للإنتحار [٢٧].

وقد طوّر الباحثون في كلية الطب في جامعة "هارفارد" خوارزمية (مجموعة من العمليات الرياضية لحلّ مشكلة ما)، لاستخدام البيانات لمئات الآلاف من الجنود، ما سمح بتحديد بعض العناصر الذين يظهرون مخاطر عالية في تنفيذ جرائم عنفية [٣٣]. ضمّ البحث بيانات متعلّقة بأكثر من 975 ألف عنصر الذين خدموا الجيش بين الأعوام 2004 و2009، مع الإشارة إلى أنّه تمّ ارتكاب 5771 عملًا جرميًا من قتل وسرقة في هذه الفترة الزمنية.

في الآونة الاخيرة، قام الجيش الأميركي بإنتاج أدوات مرتبطة بالبيانات الضخمة تسهم في وقاية العسكريين من ارتكاب جرائم عنيفة من خلال تخمين الجنود الأكثر سوءًا [٣٢].

**د- صورة عملياتية مشتركة**

تدمج الصورة العملياتية المشتركة (COP - Common Operational Picture) جميع بيانات العمليات من خلال جمعها، وربطها، واستخراج المعارف منها، واظهار النتائج في واجهة تواصل مشتركة [١٠]. تسمح التكنولوجيا المتعلّقة بالبيانات الضخمة للوحدات العسكرية من أقسام مختلفة، تبادل البيانات وتحديثها بالوقت الفعلي في الصورة العملياتية المشتركة.

**هـ- الوعي الظرفي**

تعزّز البيانات الضخمة الوعي الظرفي، وتساعد على فهم ما جرى في الماضي لفهم أوضح لأحداث الحاضر. ويجب تحليل البيانات الناجمة، عن مصادر صحيحة ودقيقة فحسب، لبلوغ الفهم الصحيح للأحداث الآنية. يُسهم استخدام أدوات البيانات الضخمة وأجهزة الاستشعار المثبّتة على الأقمار الصناعية والمحركات الأرضية والخزّانات وغيرها من المنصّات، في تعزيز الوعي بالأحداث بشكل كبير. فيولّد الدمج بين أدوات التكنولوجية المرتبطة بالبيانات الضخمة وتكنولوجيا أجهزة الاستشعار أثرًا متناغمًا.

**و- حرب الإنترنت**

ستتمكّن وكالات الإستخبارات، وبواسطة تكنولوجيا البيانات الضخمة، من التعاطي بشكل فعّال أكبر مع التهديدات السيبرانية، إذ يمكن للبيانات الضخمة أن تشكل حلًا تقنيًا استراتيجيًا للوقاية من التهديدات الأمنية، وأن تُعتبر أداة ضرورية لتحليل التهديدات السيبرانية وأنظمة الأمن.

**ز- عملية صنع القرار العسكري**

يشكّل تحليل المعلومات عن العدو بشكل دقيق وبالوقت الفعلي، إحدى الخطوات الأساسية في عملية صنع القرار العسكري[١٠]. تُظهر تكنولوجيا البيانات الضخمة قدرة على تحليل هذه المعطيات بشكل صحيح، ما يسهّل عملية اتخاذ القرار من قبل القادة العسكريين، إذ يرتكز القادة العسكريون على هذه المعطيات لوضع الخطط العسكرية المناسبة المرتبطة بخصائص الحالة الآنية والواقعية، ما يجعل القرارات العسكرية أكثر فعالية ودقّة وتحاكي التحديات التي تواجه القادة العسكريين في أرض المعركة أو الميدان.

توفّر الحسّاسات أو المستشعرات في الأجهزة العسكرية أو في البدلات العسكرية، معطيات أو صورة شاملة عن أرض المعركة للقادة العسكريين، كما تنقل الأجهزة المرتبطة بالعدو معلومات عن خصائصه وقدراته. تسمح معالجة البيانات بواسطة أجهزة مرتكزة على الذكاء الإصطناعي للقادة العسكريين، بوضع الخطط العسكرية الفعّالة والهادفة والدقيقة التي تحقق الأهداف المرجوة في الصراع مع العدوّ.

**ح- محاربة الإرهاب**

تستخدم الكثير من التنظيمات الإرهابية مثل تنظيم داعش وسائل التواصل الاجتماعي بشكلٍ كبير، إذ يعتبر عناصر التنظيم من محبي تويتر، يوتيوب، وفايسبوك وغيرها. يستخدم العناصر هذه المنصات لكسب الداعمين، وللتباهي بالأنشطة التي يقومون بها. تتّصف معظم البيانات المنشورة على وسائل التواصل الاجتماعي بالبراءة، غير أنّ تغريدة واحدة من عناصر التنظيم الإرهابي يمكن استخدامها وتحليلها. فيوفّر تحليل هذه البيانات بالوقت الفعلي، فرصةً لاستخراج المعلومات والتدخّل بشكلٍ مباشر للحد من العمليات الإرهابية. يخصّص الجيش البريطاني الكثير من الوقت لجمع كميات كبيرة من البيانات غير المنظّمة ضمن العمليات الوقائية في مواجهة الإرهاب. وتتركّز الخطوات الآتية على تحليل هذه البيانات للكشف عن المخاطر الأمنية وتهديداتها.

**ط- بيئة مشتركة للمعلومات**

يضمن نظام المعلومات المشتركة سير عمل "DoD’s Joint Regional Security Stacks" بطريقة آمنة، وتساعد تكنولوجيا البيانات الضخمة في إجراء عملية التحليل بطريقة صحيحة [٢٨].

**ي- تحليل التهديدات الداخلية**

يهدف عمل الدفاع الداخلي إلى تحديد التحديات الأمنية الداخلية والحد منها [٢٨]. تساعد البيانات الضخمة على استخدام بعض الوسائط التحليلية التي تسهّل عمليّة تحديد المخاطر الداخلية قبل أن تشكّل خطرًا كبيرًا [٢٨]. تكمن قوّة استخدام البيانات الضخمة في المجال العسكري، في القدرة على التحليل المعتمدة على نماذج فعّالة، لإنتاج دلالات رؤيوية قابلة للتنفيذ بغية تعزيز الأمن القومي.

**4. التحليل هو المفتاح**

لا تكفي البيانات الخام لتوفير دلالات رؤيوية، أو معارف واضحة تستوجب تحليلًا قويًا. فيشكّل التحليل مفتاح الكشف عن المعارف الخفية، وخصوصًا من خلال وضع الروابط والأنماط ما يسمح باستخراج التوقّعات، والدلالات العملية والخطوات التنفيذية من تدفّق المعلومات. يشكّل تحليل البيانات، بالتالي، علم فحص البيانات الخام بغية رسم الإستنتاجات ذات الأهداف الواضحة المرتبطة بالمعلومة [٣٥][٧][١٧]. ويؤسّس تحليل البيانات لأخذ القرارات الإستراتيجية لمحاربة الجرائم والإرهاب وتهديدات الأمن القومي.

يرتكز تحليل البيانات الضخمة على عاملين: البيانات الضخمة وعملية التحليل مع آلية دمج هذين العاملين لإيجاد ما يعرف بـ"الذكاء التجاري" (Business Intelligence) [٢٩]. تكمن الأهمية الكبرى لتحليل البيانات الضخمة في استنباط التقنيات والأساليب الكامنة في تحويل البيانات إلى حكمة. تسمح عملية التحليل بتطبيق أو وضع إطار (DIKW أي البيانات، المعلومات، المعارف، الحكمة) [٤٢]، وهو إطار معترف به لإدارة المعارف، ولتمثيل مستويات مختلفة لما نشاهده وما نعرفه [١١][٤٥]. يوفّر هذا النموذج من الإطار وعيًا متناميًا للمحيط. يعتمد الجيش الأميركي على إطار (DIKW) لإجراء العمليات التحليلية [٨].

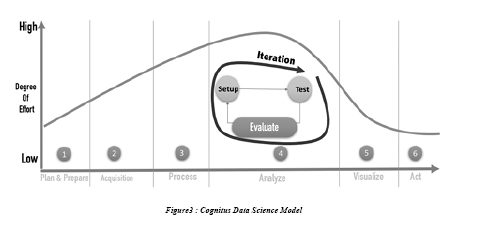
يتم استخدام أنواع عدّة من العمليات التحليلية لاستخراج المعلومات أو المعارف من البيانات، ويختلف استخدام أنواع العمليات وفق الأهداف المرجوّة.

تستخدم عملية التحليل الوصفية لتحليل بيانات من الماضي لمعرفة ما حدث. فعلى سبيل المثال، يساعد استخراج المعارف من البيانات المرتبطة بحرب العراق في العام 1991 وتحليلها, على إيجاد الأنماط أو الاستراتيجيات التي أسهمت في فوز الجهة الرابحة. يجيب التحليل التشخيصي أو ما يعرف بالتحليل السببي على سؤال: لماذا حدث هذا الأمر. أما التحليل التنبئي، حيث تؤدي البيانات الضخمة دورًا مهمًا في هذا المجال، فيسمح بتوقع الأحداث التي يمكن أن تحدث في المستقبل. مثلًا، يمكن تحليل البيانات من مصادر مختلفة: المدوّنات، وسائل التواصل الاجتماعي، الجرائد الإلكترونية وغيرها لتخمين حصول عمل إرهابي. ويهدف التحليل التوجيهي إلى إيجاد مقترحات في شأن موجبات العمل في بعض الحالات، مثل الخطوات التي يجب اتخاذها لتفادي حدوث عمل إرهابي.

تسهم البيانات الضخمة في تعزيز استخدام علم البيانات وهو علم معاصر يسمح بتحويل البيانات إلى أفعال. يدعم هذا المجال منطقا الاستقرائي (Inductive) و الاستنباطي (Deductive) لاستخراج دلالات تنفيذية من كميّة هائلة من البيانات المبنيّة وغير المبنيّة.

يعتبر علم البيانات (Data Science) متعدّد التخصصات, إذ يتضمّن المبادئ، والآليات، والتقنيات المتعدّدة المرتبطة بعلم الحاسوب ومنها ما هو متّصل بالآلة، قاعدة البيانات، التعلّم، والتدقيق. ويستثمر المجال الأدوات الرياضية والإحصائية لتطوير نماذج يمكن استخدامها في عمليّة تحليل البيانات واتخاذ القرارات المرتكزة على البيانات.

تـتألّـف عـمـلـية تحليـل الـبـيانـات مـن مـراحـل مـخـتـلفـة. ويـوفّـر عـلـم البيانات نماذج لتطوير عملية التحليل ومنها: Hammerbacher Model وBooze-Allen Model. ويقترح المركز الفرنسي "COGNITUS" للبحث والتطوير في مجال تحليل البيانات الضخمة، نموذجًا شاملًا يعتمد على الكثير من النماذج الحالية. (يبيّن الرسم 3 النموذج).



يتضمّن النموذج ست مراحل: تبدأ عملية التحليل بالتخطيط وتحضير الأسئلة وفق الهدف. تساعد هذه الأسئلة على تحديد مصادر البيانات المطلوبة لعملية التحليل. في المرحلة التالية، يتم استخدام البيانات وفق نمطين: الوقت الفعلي أو على دفعات. ففي نمط الوقت الفعلي، تتدفّق المعلومات من المصادر مثل أجهزة الاستشعار أو المجسّات أو التطبيقات، بينما يتم جمع البيانات في النمط الثاني من المصادر كل أربع وعشرين ساعة. وتتضمّن المرحلة التالية تنظيف البيانات، دمجها، تحويلها وما إلى ذلك. ويمكن إجراء هذه العملية في الوقت الفعلي (تتمّ العملية بشكل مباشر) أو على دفعات (أي أنّ التحليل يتمّ بشكل دوري). ويتمّ استخدام نماذج مختلفة في النمطين. هذا وتشكّل مرحلة التحليل المرحلة الأكثر دقّة، وبما أنّ هذه العملية تفاعلية، فيتكرّر إجراء التقويم مع توافر بيانات جديدة. تسمح عملية إظهار النتائج بطريقة شاملة وتفاعلية للمستخدمين بتداولها بشكل سهل. أمّا المرحلة الأخيرة فتكمن في التدخل أي أنّ صنّاع القرار يتّخذون الإجراءات الضرورية مثل توقيف أحد المشتبه بهم في التورّط في عملية إرهابية.

**5. تحليل البيانات العسكرية**

بعد الهجمات التي شهدتها الولايات المتحدة الأميركية في الحادي عشر من أيلول، أصبحت الإستخبارات الأميركية بحاجة أكبر إلى دمج مختلف البيانات. غير أنّ البيانات بشكلها الخام تحتاج إلى التحليل للكشف عن المعلومات والمعارف الخفية، وهناك أنواع عدّة من تحليل البيانات المتعلقة بالشؤون العسكرية.

**Modus Operandi**

تمّ تصميم "Modus Operandi" لمنح القوات المرتكزة في الخطوط الأمامية القدرة على تحديد عدد الأشخاص، والتنظيمات، والأماكن والأحداث وترابطها بالخطوط الزمنية [٢٠]. يتمّ استخدام تكنولوجيا البيانات الضخمة مثل: "Hadoop"، بيانات الرسم البياني، وما إلى ذلك لإستخراج الدلالات المرتبطة بـ"لايكات" الفايسبوك في شأن حياة الأشخاص الأشرار [٢٠]. يعمل تصميم "Modus Operandi" على دمج البيانات الضخمة بالخبرات المعرفية لوضع الإطار المناسب لتحديد مختلف الأنماط، واستخراج بعض التصورات مثل الخرائط، والخطوط الزمنية [٣٩].

**Wave**

يعتمد "Wave" على تطبيقات "Hadoop" مثل "HBase" و"Accumulo" و"Cloudbase", لإدراج كميّات عديدة من البيانات المنظمة في النظام، وفي الخوارزميات لإضافة معنى على الكلمات والتعابير الإنسانية [٢٠]. ويمكن أن يعود تدفق البيانات إلى مصادر مختلفة مثل التقارير، تعليقات وسائل التواصل الاجتماعي، الأخبار، البيانات المرتبطة بالمصارف أو بالحكومات. يعمل التصميم على هندسة هذه البيانات وتحويلها إلى رسوم بيانية  تسمح للمستخدمين بإيجاد الروابط بين الأشخاص، والتنظيمات والأحداث والأمكنة والتي يصعب عادة ربطها بشكل تقليدي. مؤخرًا، أطلق "Wave" واجهة التواصل "Blade" التي تسمح بتفاعل أسهل مع المستخدمين. يوفر "Blade" تقنية "SPARQL" لكتابة الاستفسارات وتنفيذها.

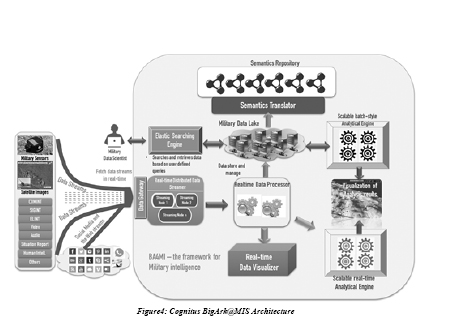
**Oorah Hadoop**

يدمج "Oorah Hadoop" بين ميزات "Modus Operandi" و"Wave"، ويسمح بجمع البيانات من قواعد البيانات والرسائل. يتمّ الإعتماد على "wave" لجمع البيانات بينما يتم استخدام "Modus" لتحليلها، ويتم اظهار النتائج على شكل خرائط أو رسوم بيانية.

وعلى الرغم من أنّ تحليل البيانات العسكرية في الوقت الفعلي يرتكز على مراجعة الإنتاج الفكري والمدوّنات، غير أنّ المعطيات الحالية تفتقر إلى أدوات تحليلية في الوقت الفعلي، فتعتمد الحلول القائمة على تصميمات "Hadoop" و"Map Reduce" التي لا يمكن من خلالها إجراء تحليل بالوقت الفعلي. وتظهر هذه الدراسة أنّ هذه التصميمات غير مناسبة لإجراء تحاليل تنبئية في المستقبل التي تشكًل مفتاحًا لاستثمار البيانات الضخمة. فعلى سبيل المثال، يساعد التحليل التنبئي على تنبؤ أو توقّع أهداف التطرّف (من جماعات وأفراد)، أو تحديد الأنماط. فبالتالي، تفتقر المعطيات الحالية الى حلول مرتبطة بالتحليل التنبئي وبالتحليل بالوقت الفعلي، اللذين يشكّلان أدوات ضرورية للإستفادة من البيانات الضخمة في الشؤون العسكرية.

**٦- نظام متخصص للذكاء الاستخباراتي**

يشكّل نظام "COGNITUS-BigArk@MIS, Military Intelligence System"، كما يظهر الرسم4، حلًا متخصصًا، ذا أداء عالٍ، قابل للتطوير لمعالجة محدودية أداء التقنيات التكنولوجية المذكورة سابقًا. طوّر المركز الفرنسي لتحليل البيانات الضخمة "COGNITUS" هذا النظام لتوفير حلول سهلة بكفاءة عالية مرتبطة باستخدام البيانات الضخمة ونماذج انترنت الأشياء لرصد التهديدات المحتملة للأمن القومي. ويعتبر هذا النظام حلًا فعًالا يوفّر عمليات تحليل في الوقت الآني والحقيقي (real-time) وبدفعة واحدة. وبالتالي يسمح النظام بالتحليل بدفعة واحدة وعلى نطاق واسع البيانات المخزّنة في "Military Data Lake" الذي يشكّل جزءًا من "BigArk@MIS". ويسمح النظام، أيضًا، بتحليل البيانات في الوقت الآني.



يمكن لـ"BigArk@MIS" أن يجمع البيانات من مصادر مختلفة ومتعدّدة ومنها: أجهزة الاستشعار، وسائل التواصل الاجتماعي، الصحف، أنظمة المعلومات العسكرية وغيرها.

تسمح بوابة "BigARK@MIS" بالوصول إلى البيانات الواردة حيث تتمّ معالجة البيانات وإرسالها إلى ثلاثة مكوّنات مختلفة: بحيرة البيانات (data lake) لتخزينها، المصوّر الآني (real-time visualizer) لمسح شامل للبيانات، ومحرّك تحليل البيانات في الوقت الآني. يحصل محرّك تحليل البيانات على المعطيات من "بحيرة البيانات" ويضع تصويرًا للنتائج من خلال المصوّر الآني.

يشكّل "semantic repository" أحد المكوّنات الأساسية لـ"BigArk@MIS" ويخزّن البيانات التي تتم ترجمتها بواسطة مترجم الاستدلال. ويسمح الاعتماد على البيانات المرتبطة للمستخدمين بفهم دلالات البيانات والكشف عن الدلالات الخفيّة. في المقابل، لا تسمح نماذج البيانات التقليدية بالكشف عن دلالات البيانات واستخراجها. يكشف المحرّك المنطقي عن العلاقات الخفية والمموّهة التي تخبئها البيانات ما يمكّن المستخدمين من استخراج المعاني المفيدة من البيانات، فيتفرّد نظام "BigArk@MIS" بهذه القدرة المميّزة أو الفريدة.

**7- الإستنتاج**

شهدت السنوات الخمس الأخيرة نموًا جذريًا في البيانات الضخمة نسبة إلى زيادة استخدام إنترنت الأشياء في بناء الأنظمة المترابطة مثل الأنظمة العسكرية الذكية، وإلى ارتفاع عدد التطبيقات المتعلّقة بوسائل التواصل الإجتماعي من نصوص، وصور، وتسجيلات صوتية وفيديو. تؤمّن هذه البيانات الضخمة فرصًا عدّة للصناعة العسكرية، خصوصًا أنّ تحليل البيانات الضخمة يسمح بالكشف عن دلالات تنفيذيّة تمكّن صنّاع القرار من الارتكاز عليها لتطوير مختلف الشؤون العسكرية. تساعد البيانات الضخمة على تطوير قدرات الإستخبارات العسكرية من خلال جمع البيانات من مصادر مختلفة وبناء منصّة حاسوبية مترابطة تعزّز تبادل المعلومات بين العسكريين. في هذه الدراسة، تمّ تسليط الضوء على الوعود التي تظهرها البيانات الضخمة في المجال العسكري، وخصوصًا مختلف استخدامات البيانات الضخمة في الإستخبارات العسكرية.

ارتكزت هذه الدراسة على تسليط الضوء على أدوات تحليل البيانات الضخمة ومنها على سبيل المثال "Modus Operandi". تبيّن هذه الدراسة مقارنة للحلول الحالية المعتمدة على تكنولوجيا البيانات الضخمة  من دون أن توفّر هذه الحلول معالجة البيانات في الوقت الفعلي، ما يشكّل تحديًا لصانعي القرار لاتخاذ القرار في الوقت الفعلي. لذا تطرح هذه الدراسة تصميمًا واعدًا يعالج محدوديات الحلول الحالية، إذ يسمح بالتقاط البيانات ودمجها وتحليلها في الوقت الفعلي، ما يسمح لصانعي القرار الفرصة باتخاذ القرار المناسب في الوقت المناسب. من ناحية أخرى، يعتبر نظام "BigArk@MIS" أداةً واعدة بميزات وخصائص جديدة وفعّالة لمعالجة النواقص أو المحدودية التي تظهرها الأدوات الأخرى.

وأخيرًا لا بد من الإشارة إلى أنّه وعلى الرغم من أنّ البيانات الضخمة واعدة في المجال العسكري، غير أنّ دولًا قليلة تعتمدها نسبة إلى أنّ تكنولوجيا البيانات الضخمة معقّدة وتحتاج إلى خبرات عالية وكفوءة، ما يوجب تسهيل هذه التكنولوجيا وتبسيطها لرفع معدّل استخدامها.

**المراجع:**

[1] Big data: 20 mind-boggling facts everyone must read. http:c//www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#4deef79d6c1d. Accessed: 2016-10-05.

[2] Cern computing. Available Online: https://home.cern/about/computing.

Date Accessed: 2016-10-05.

[3] A comprehensive list of big data statistics.

Available Online http://wikibon.org/blog/big-data-statistics/. Accessed: 2016-10-05.

[4]Gartner hype cycle: A framework for describing the emergence of new technologies.

 http://declineofscarcity.com/?p=254. Accessed: 2016-10-05

[5] What is big data? Available Online: http://www.gartner.com/it-glossary/big-data/. Date Accesed: 2016-10-05

[6] P. Andersen. What is Web 2.0?: ideas, technologies, and implication.

[7] M. Barlow. Real-Time Big Data Analytics: Emerging Architecture. " O'Reilly Media, Inc.", 2013.

[8] J. P. Carlisle. Escaping the veil of maya: Wisdom and the organization. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), volume 7. IEEE, 2006.

[9] M. Chui, M. Lo\_er, and R. Roberts. The internet of things. McKinsey Quarterly, 2(2010):1-9,2010.

[10] H. Cintiriz, M. Buhur, and E. Sensoy. Military implications of big data. In International Conference on Military Security Studies, ICMSS-2015, Turkey, Istanbul, War Colleges Command, 2015.

[11] H. Cleveland. Information as a resource. Futurist, 16(6):34-39, 1982.

[12] C. Downing. System of system common operating environment sw. http://mil-embedded.com/articles/the-internet-thingsthe- intelligence-community/.

[13] M. HARIDAS. Redefining military intelligence using big data analytics. 2015.

[14] http://data-magnum.com/how-many-vs-in-big-datathe- characteristics-that-de\_ne-big data/. How many. Accessed: 2016-10-06.

[15] Data Economy. Us military using big data to improve situational awareness. Available Online: http://dataconomy.com/us-military-using-big-dataimprove- situational awareness/. Accessed: 2016-10-08.

[16] Amazon Web Service. The internet of things for military. Available Online: https://csis-prod.s3.amazonaws.com/s3fs public/. Accessed: 2016-10-08.

[17] Search management. Data analytics. Available Online :

http://searchdatamanagement.techtarget.com/de\_nition/data analytics. Date Accessed: 2016-10-06.

[18] The Big Data Institute. Big data definition. Available Online: https://thebigdatainstitute.wordpress.com/2013/04/21/bigdata de\_/. Date Accessed: 2016-10-06.

[19] Cisco. Internet of everything for defense. Available Online: https://www.cisco.com/c/dam/. Date Accessed: 2016-10-11.

[20] Datanami: SasS for military intelligence. Available Online : https://www.datanami.com/2014/02/03/. Date Accessed: 2016-10-11.

[21] LinkedIn. Leverage the IoT for a more efficient military. Available Online: https://www.linkedin.com/pulse/leverage-iot-moree\_cient-military-a-white-paper-tom kenslea Date Accessed: 2016-10-11.

[22] Microsoft. Improving military effectiveness with IoT. Available Online: ] https://www.microsoft.com/en-us/cloudplatform/ internet-of-things-azure-iot suite. Date Accessed: 2016-10-11.

[23] Rusi. Big Data Report. Available Online: https://www.rusi.org/downloads/assets/. Date Accessed: 2016-10-11.

[24] SemiWiki: The Internet of Things for Military. Available Online: https://www.semiwiki.com/forum/content/4004-whatdoes-ford-mustang-intelmotors.html. Date Accessed: 2016-10-11.

[25] Statistitia. Available Online: https://www.statista.com/statistics/256235/totalcumulative- number-of-tumblr blogs/.Date Acessed: 2016-10-03

[26] Stanford Big Data Report. Available Online: http://web.stanford.edu/group/mmds/slides2012/sfahey.pdf. Date Accessed: 2016-10-11.

[27] Apa. Big data help prevent army suicides. Available Online: http://www.apa.org/monitor/2015/04/armysuicide.aspx. Date Accessed: 2016-10-11.

[28] C4ISRNET. Dod's big bets on big data. Available Online: http://www.c4isrnet.com/story/military-tech/blog/business-viewpoint/2015/08/25/dods-big-bets-big-data/32321425/. Date Acessed: 2016-10-11.

[29] http://www.cloudtalk.it/wp content/. Big data data analytics.

Date Accessed: 2016-10-06

[30] http://www.ey.com. Big data changing the way businesses compete and operate. Accessed: 2016-10-06.

[31] http://www.forbes.com/sites/techonomy/. Military intelligence rede\_ned:

Big data in the battle-field. Date Accessed: 2016-10-11.

[32] Independent. The US military exploring 'big data' to prevent violent crimes by soldiers before they happen. Available Online: http://www.independent.co.uk/news/world/americas/usmilitary-exploring-big-data-to-prevent-violent-crimesby-soldiers-before-they-happen a6691036.html. Date Accessed: 2016-10-11.

[33] Los Angeles Times. New tool can identify soldiers most likely to commit violent crimes, study shows. Available Online: http://www.latimes.com/science/sciencenow/la-sci-snpredicting- violent-crime-by-army-soldiers20151006-story.html. Date Accessed: 2016-10-11.

[34] Meta Build. System of system common operating environment sw. Available Online: http://www.metabuild.co.kr/. Date Accessed:2016-10-11.

[35] Big data analytics advanced analytics in oracle database. Available Online: http://www.oracle.com/technetwork/database/options/advancedanalytics/bigdataanalyticswpoaa1930891.pdf. Accessed: 2016-10-07.

[36] SaS Software. SasS for military intelligence. Available Online:

http://www.sas.com/resources/brochure/militaryintelligence overview.pdf. Date Accessed: 2016-10-14.

[37] Tempered Network: Securing the federal internet of things with micro-segmentation. Available Online: http://www.temperednetworks.com/securing-thefederal- internet-of-things-with-microsegmentation/. Accessed: 2016 10-14.

[38] The Free Dictionary. Available Online: http://www.thefreedictionary.com/Unmanned+Aerial+Vehicle. Date Accessed: 2016-10-18.

[39] S. Kulshrestha. Big data in military information & intelligence. IndraStra Global, 2016.

[40] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. H. Byers. Big data: The next frontier for innovation, competition, and productivity, 2018.

[41] M. Schroeck, R. Shockley, J. Smart, D. Romero-Morales, and P. Tufano. Analytics: The real-world use of big data. IBM Global Business Services, pages 1-20, 2012.

[42] R. P. Schumaker. From data to wisdom: The progression of computational learning in text mining. Communications of the IIMA, 11(1):4, 2014.

[43] P. B. Symon and A. Tarapore. Defense intelligence analysis in the age of big data.

[44] F. Xia, L. T. Yang, L. Wang, and A. Vinel. Internet of things. International Journal of Communication Systems, 25(9):1101, 2012.

[45] M. Zeleny. Management support systems: towards integrated knowledge management. Human systems management, 7(1):59-70, 1987.

[46] Military Intelligence Redefined: Big Data in the Battlefield. http://www.forbes.com/sites/techonomy/2012/03/12/military-intelligence-redefined-big-data-in-the-battlefield/#377992e8718f.

**Big Data for Military Intelligence**

The unprecedented growth of data volume, variety, and velocity gave rise to the notion of Big Data which promoted extensive opportunities for various domains including military intelligence. Modern technologies such as Internet of Things (IoT) led to radical changes in military information systems. Various smart objects such as smart weapons have been manufactured in the last few years. In fact, IoT is changing the conventional military landscape. Additionally, the external sources such as social medias have become critical to intelligence agencies because they are widely used by extremist network that is spanned over the globe. The data produced by IoT and social media applications (e.g., Twitter and Facebook) provide an opportunity to perform deep and wide analysis to extract actionable insights, which assist in fighting against terrorism or enemy states. However, an efficient analysis with Big military data is non-trivial because Big Data fosters several challenges that concerns size, speed, and variety of data.

There are a few solutions such as Modus Operandi for military data analytics; however, an efficient solution for real-time data analysis is missing in state of the art. Additionally, there is no predictive analytics for military intelligence.  These shortcomings revealed the requirements of an efficient analytics, which can perform analysis in, real-time. In this paper, we discuss different aspects of Big Data and its role in military intelligence. We explore state of the art technologies and outline their shortcomings. In addition, we propose, BigArk@MIS, a novel big data based system for real-time military intelligence.

**Le Big Data dans les renseignements militaires**

7 milliards d’être humains dans le monde, 2,5 milliards d’internautes dont 1,9 milliard sont présents sur les réseaux sociaux, 6,5 milliards de téléphones, 10 milliards d’objets connectés. Chaque jour, Google traite 24 péta-octets de données. 350 millions de photos sont chargées sur Facebook, 400 millions de tweets sont envoyés; 100 heures de vidéo sont mises en line chaque minute sur YouYube. Ces chiffres sont impressionnants. Plus impressionnant encore est le rythme auquel ces chiffres croissent. Il s’agit de l’ère de Big Data. Pour ne pas être submergé par ce déluge de données, il a fallut développer des nouveaux outils, capables de traiter plus rapidement ces données de natures très variées, dispersés, et parfois extrêmement volumineuses. Le Big Data est souvent associé au traitement de très gros volumes de données. Ce n’est pas tant la quantité qui est déterminante, mais l’association dans une même analyse de données variées afin d’en déduire des informations qu’il aurait été impossible de mettre en évidence avec les analyses classiques de données structurées. L’utilisation du Big Data ouvre de nouveaux horizons, de nouvelles opportunités pour les acteurs de différents secteurs allant des secteurs de service public, santé, éducation, télécommunication, énergie, renseignement, aux secteurs de commerce, énergie, banque et assurance, etc.

Dans ce papier, nous nous focalisons sur l’utilisation du Big Data dans les renseignements militaires. En effet, divers objets intelligents comme les armes intelligentes ont été fabriqués au cours des dernières années, ce qui contribue au changement du paysage militaire conventionnel. Les données produites par les objets connectés et les réseaux sociaux (par exemple, Twitter et Facebook) fournissent l'occasion d'effectuer une analyse approfondie et avancée pour extraire des informations de valeur, ce qui aide à lutter contre le terrorisme ou les États ennemis. Cependant, une analyse efficace de ces données s’avère assez difficile car le Big Data favorise plusieurs défis liés au volume, à la vitesse et à la variété des données.

A nos jours, il existe quelques solutions telles que Modus Operandi pour l'analyse des données militaires. Cependant, les solutions existantes souffrent des limites sérieuses quand il s’agit d’une analyse en temps réel ou une analyse prédictive des données militaires. Pour pallier à ces limites, nous proposons BigArk@MIS, un nouveau système à base des technologies Big Data, permettant une analyse en temps réel et prédictive des données militaires.

- See more at: https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B6%D8%AE%D9%85%D8%A9-%D9%81%D9%8A-%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%AE%D8%A8%D8%A7%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B9%D8%B3%D9%83%D8%B1%D9%8A%D8%A9#sthash.COEfI1Re.dpuf