الافتتاحيّة

المدير العام
اللواء عباس ابراهيم

حصانة الأمن الرقمي*

لأن الحديث عن السيادة والاستقلال والامن الوطني لم يعد ممكنا من دون الاخذ جديا في الاعتبار موضوع الامن السيبراني، لا بد من التوقف مليا وبعناية شديدة امام الاخطار البالغة الدقة التي يشكلها الامن الرقمي التي تُضاف الى مجموعة اخطار منطلقة من منصتي العدوين الاسرائيلي والتنظيمات الارهابية، اللذين لا يزالان يضربان لبنان ونتصدى لهما بطاقاتنا القصوى.

لا اخفيكم سرا ان الوقائع اثبتت الحاجة الملحة الى ايلاء هذا الشق الامني عناية استثنائية لحماية الدولة ومؤسسات القطاعين العام والخاص والمرافق الحيوية، وقبل كل شيء، حماية حياة اللبنانيين وحرياتهم الخاصة. العكس من ذلك، يعني ان السيادة الوطنية من دون حصانة الامن الرقمي منقوصة.

كشف العقد الاخير دول العالم برمتها امام خطر الامن السيبراني، وسرعة تطور آلياته القادرة على شل قطاعات كاملة في الدولة والاسواق واعطابها، ناهيك بأن الجرائم الالكترونية الى ارتفاع مستمر، في ظل عجز الامن في معناه المادي البحت والتقليدي عن كبحه. كلما انخرط العالم في الفضاء الالكتروني، وهو مضطر الى مواكبته والانخراط فيه كي يتماشى مع العصر والاقتصادات الحديثة، ارتفعت معدلات الاخطار والحروب الناتجة من الهجمات السيبرانية.

قد لا يحتاج التدليل على هذا الخطر الى عناء كبير، في ظل الحديث والوقائع الثابتة عن بلوغ هذا الخطر الى حد التأثير على اراء الناخبين وتعديل نتائج الانتخابات في هذا البلد او ذاك، ما اثر على جوهر الديموقراطية ذاتها وما تضمنه من استقرار. كلنا يدرك ان هذا الخطر صار يهدد خصوصياتنا وحرياتنا الشخصية وحتى حق الملكية المقدس في النظم السياسية التي تعتنق مذهب الحريات الاقتصادية. كل ما هو قاعدة بيانات (داتا) صار هدفا يتراوح بين حدي الابتزاز المادي او الاستيلاء والتدمير.

امام هذا الواقع يصبح كل فرد عرضة للاستهداف ما دام يستعمل الهاتف الذكي او الكومبيوتر. لذلك فإننا معنيون، لا بل ملزمون، حماية مؤسساتنا وقطاعاتنا وخصوصياتنا التي تنتشر في فضاء الانترنت. هذا الالتزام يرتقي الى حد الواجب، في ضوء الهجمات والخروقات الإسرائيلية السيبرانية المنظمة التي تشن على لبنان كله ومن دون تمييز. كذلك الامر في ظل ما نجحت في تحقيقه المنظمات الارهابية لجهة تطويع انتحاريين وشبكات وخلايا، مهمتها تعميم الخراب والقتل واسقاط الدولة اللبنانية على خط النار الممتد من سوريا حتى ليبيا. نحن في هذا الصدد اسقطنا واحبطنا ـ ولا نزال ـ العشرات من الشبكات التي تسعى يوميا الى تجنيد عملاء للعمل لصالح العدو الاسرائيلي. وهي الحرب الاخطر التي نخوضها في ايامنا هذه.

يوما بعد يوم، يتأكد لنا وجوب ايلاء الامن السيبراني ما يستلزمه من عناية ضرورية لحماية الحواسيب، الخوادم servers، الهواتف الذكية، الانظمة الإلكترونية، الشبكات والمعلومات من الاعتداءات والهجمات الرقمية التي تتخذ اشكالا عدة مثل البرمجيات الخبيثة malware، التصيد phishing، هجمات التطبيقات application attacks، هجمات الفدية ransomware، وهي تستهدف ممتلكات سياسية، عسكرية او البنية التحتية للدولة، كما تستهدف الافراد والشركات غالبا للحصول على معلومات سرية او لدافع مادي.

جزء كبير من الحروب اليوم تشن على الفضاء السيبراني، وعبر نسخ معلومات وسرقتها، او تعطيل انظمة شديدة الحساسية. صار كافيا ان تشن حكومة ما هجمة سيبرانية منظمة لاختراق قاعدة عسكرية عند دولة تفترضها هي عدوها، لترد الاخيرة بحرب عسكرية او امنية. الاكثر سوءا في هذا الاطار ان مجموعات صغيرة ولاهداف ايديولوجية، او افرادا مميزين بمهارات رقمية، صاروا قادرين في الحد الادنى على ضرب اساسات مؤسسات تشكل نظما اقتصادية وتجارية، وكحد اقصى احداث قلاقل واسعة النطاق قد تتطور وتأخذ صفة اضطرابات اقليمية او دولية. بين الامرين امست سيادة اي دولة في حاجة الى اعتبار الامن السيبراني ركنا في عقيدتها الامنية.

بحسب الاحصاءات الموثوق بدراستها وعلميتها ودقتها، جاء لبنان في المرتبة المتقدمة عالميا لجهة تعرضه لهجمات سيبرانية، خصوصا لجهة استهداف اشخاص تعرضوا لعمليات اختلاس البيانات المصرفية الخاصة بهم، من خلال ما يسمى «Mobile banking Trojans»، وهي برامج مخصصة للولوج الى اجهزة الخلوي والكومبيوترات وتتضمن قدرات تقنية عالية وتسمى "احصنة طروادة" نسبة الى حصان طروادة التاريخي.
هذا الواقع يستدعي ورشة تقنية تعتزم المديرية العامة للامن العام الشروع في اطلاقها وفقا لما تجيزه الصلاحيات، وفي اطار الالتزام الكامل والحرفي بالنص القانوني لجهة حماية الحريات، وذلك عبر تخصيص شعبة تحدد علميا مخاطر الامن السيبراني، من خلال اعتماد افضل المعايير الدولية لتقييم المخاطر، وتوسيع قاعدة تبادل المعلومات ومؤشرات التهديد المتعلقة بالامن الوطني مع سائر المؤسسات الامنية اللبنانية.
التلكؤ عن هذا الواجب يعني قبولا باستباحة السيادة الوطنية، وانتهاكا لحرية اللبنانيين وخصوصيتهم. ما يجب التأكيد عليه في هذا الاطار ان النجاح يبقى رهنا بحسن التوظيف والتدريب والتعليم التقني والفني، على ان تولي الوزارات المعنية عنايتها القصوى لمناهج التعليم الرقمي، كون الذكاء الصناعي والتجاري والعلمي لا يمكن مواكبته بالمناهج القديمة والبرامج المعمول بها. عالم الانترنت لا يرحم قليلي الخبرة والمهارات الالكترونية. كما ان الاقتصاد القوي صارت قاعدته الاساس تقوم على المعرفة الرقمية.

ليس خافيا على احد، ولا هو مبالغة القول ان صناعة كاملة في عالمنا الحديث تقوم على تطوير المهارات البشرية لتتكيف بازاء الخطر السيبراني، لكن دائما ثمة شيء ما يستدعي التوقف عنده، ألا وهو كيف يستطيع المهاجمون الالكترونيون استباق برامج التطوير ما يساعدهم على النجاح؟ تقديري للجواب هو ان المهاجمين يعرفون ما يريدون، في مقابل مُستهدَفين لا يعرفون امرا من اثنين او كليهما معا: ماذا يواجهون، او كيف يدافعون؟ في الحالين يستدعي منا كمسؤولين في شتى الميادين الاستثمار بـ"السلامة السيبرانية" او "السلامة الالكترونية"، بما يمكننا من ادعاء تحقيق "الامن المعقول"، لأن لا امن مثاليا في عالم تحكمه شهيات مفتوحة للسيطرة والتحكم ومنه عدوّان ما توقفا للحظة عن استهداف لبنان هما: اسرائيل والتنظيمات الارهابية.

---

* كلمة المدير العام للامن العام اللواء عباس ابراهيم في المؤتمر الذي نظمته المديرية العامة للامن العام تحت عنوان: "توعية المواطنين على المخاطر الاسرائيلية عبر الفضاء السيبراني، ودورها في تجنيدهم لصالح اعداء الوطن" في 27 حزيران 2018.