**الحرب الإلكترونية**

[**العدد 118 - تشرين الثاني 2021**](https://www.lebarmy.gov.lb/ar/content/118-d)

**الحرب الإلكترونية**
إعداد: العميد علي قانصو
مدير التوجيه

في العصر الحديث، لم يعد خوض الحروب مقتصرًا على الوسائل القتالية التقليدية المتعارف عليها، مثل الأسلحة الفردية المختلفة والمدرعات والطائرات والسفن الحربية وغيرها. ولم يعد مسرح الحرب محصورًا ببقعة جغرافية تُرسَم على أساسها خطط الهجوم والدفاع وتحرُّك الوحدات.

باتت الحروب بين الدول تُخاض في ميدان جديد هو الميدان الإلكتروني، المسمى أيضًا السيبراني، إذ فَتَحَ التطوّر التقني والرقمي مجالات لم تعهدْها البشرية من قبل، بفعلِ توسُّعِ شبكاتِ الاتصال ودخولِ المعلوماتية في كل جانب من جوانب الحياة.

فكما أن الدول تُجهّز جيوشها وتُدرّبها وتؤمّن لها السلاح والعتاد اللازم للقيام بواجباتها، تسعى كذلك إلى تعزيز جهوزيتها الإلكترونية صونًا لمنشآتها ومواقعها من الاختراق والتخريب. وكما أن الاعتداءات الإرهابية تُرتَكَب بالأسلحة والأحزمة والعبوات الناسفة والسيارات المفخخة، فهي تُنَفَّذ من خلال حسابات التواصل الاجتماعي ومواقع الإنترنت، وتَستهدف الفِكرَ لا الجسد، وتعمل على اجتذاب الأشخاص، ولا سيما الشباب، للوقوع في شباك العنصرية والتطرف.

وأكثر ما يعنينا هنا كمؤسسة عسكرية، التهديد الإلكتروني من جانب العدو الإسرائيلي والمجموعات الإرهابية التي دأبْنا على التصدي لها منذ سنوات. فالعدو الإسرائيلي يستخدم الفضاء الرقمي كوسيلة إضافية للتجسس والحصول على المعلومات، واستدراج اللبنانيين وتجنيدهم كعملاء من حيث لا يعلمون. أما الإرهاب، فيَنْشَط كذلك لِبَثّ الفتنة بين المواطنين، وتحريض ضعاف النفوس على الجيش، ودفْعهم إلى الانخراط في صفوف التنظيمات الإرهابية وتحويلهم إلى آلاتٍ للقتل والدمار.

يستلزم هذا الوعيَ والمعرفةَ على عدة مستويات، أولها على مستوى المجتمع بصورة عامة، فينبغي تثقيف الشباب حول خطورة الجيوش الإلكترونية المعادية، وتحذيرهم من الأعداء المتربصين خلف حسابات وسائل التواصل، وكثير منها وهمي. أمّا المؤسسات الأمنية وعلى رأسها الجيش، فتقع عليها مسؤولية كبيرة في حماية أفرادها أولًا من أي خرق عبر الوسائل المذكورة، وملاحقة أعداء الوطن ثانيًا وإحباط خططهم في الفضاء السيبراني، مثلما تتم ملاحقتهم واعتقالهم على أرض الواقع. وإن الإنجازات التي حققتْها المؤسسات المذكورة في هذا النطاق واضحةٌ بيّنة عبر الكثير من العمليات الأمنية التي تُنجَز بناءً لجهود الفرق المتخصصة بالأمن الإلكتروني.

ما زال أعداء الوطن ماضين في مخططاتهم لضرب وحدتنا وسلمنا الأهلي. وفي المقابل، ما زال الجيش كما باقي المؤسسات الأمنية حاضرًا في جميع الساحات لإفشال تلك المخططات وسَوق المتورطين فيها إلى العدالة. ويبقى الانتماء الوطني السليم وسِعَة الثقافة والاطّلاع ضرورةً لا غنى عنها لأبنائنا في سبيل استكمال تحصين المجتمع، وإغلاق جميع الثغرات التي تهدّد استقراره.

**Cyberwarfare**

In modern times, warfare is no longer limited to traditional means of combat, such as various individual weapons, armored fighting vehicles, aircrafts, warships and others. The theater of war is no longer confined to a geographic region where attack and defense are planned, and unit movements are mapped out.

Wars between countries are now being fought in a new field, “the electronic field”, also called cyberspace.  The technical and digital development has opened up areas that humanity has never known before, due to the expansion of communication networks and the integration of informatics in every aspect of life.

Just as countries prepare and train their armies and provide them with the necessary weapons and equipment to carry out their duties, they also seek to enhance their electronic readiness to protect their facilities and sites from being hacked and sabotaged. Just as terrorist attacks are committed with weapons, explosive belts, improvised explosive devices and car bombs, they are carried out through social media accounts and Internet sites. They target the thoughts, not the body, and work to attract people, especially the young ones, to fall into the trap of racism and extremism.

What concerns us most here as a military institution is the cyber threat from the Israeli enemy and the terrorist groups that we have been confronting for years. The Israeli enemy uses digital space as an additional means to spy, obtain information, and lure the Lebanese and recruit them as agents. As for terrorism, it is also active to sow discord among citizens, incite weak-minded individuals against the Lebanese Army, push them to join the terrorists, and turn them into killing machines.

This requires awareness and knowledge on several levels, the first is the level of society in general, where young people should be educated about the danger of hostile electronic armies, and warned about the enemies lurking behind social media accounts, many of which are fake. As for the security institutions, especially the Lebanese Army, they bear a great responsibility to protect their troops first from any violation through the aforementioned means, and second to pursue the enemies of the homeland and thwart their plans in cyberspace, just as they are pursued and arrested on the ground. The achievements made by the mentioned institutions in this field are clear and evident in many security operations, carried out through the efforts of the specialized electronic cybersecurity teams.

The enemies of the homeland are still going ahead with their plans to strike our unity and civil peace. In return, the Lebanese Army, like the rest of the security institutions, is still present in all arenas to thwart these plans and refer those involved to the competent judicial authorities. National loyalty, rich culture and knowledge remain an indispensable necessity for our children to protect their society and close all gaps that threaten its stability.