



L'armée de terre a testé en 2015 une messagerie cryptée mise au point par PolSys.

Une messagerie sécurisée sur le champ de bataille

Les militaires s'intéressent déjà à la cryptographie post-quantique. Avidé d'utiliser les dernières technologies de communication, l'armée de terre française avait souhaité tester sa faisabilité dans le cadre d'une expérimentation menée fin 2015 mobilisant une centaine de soldats. Après plusieurs mois de développement spécifique, le laboratoire PolSys, commun à l'Institut national de recherche en informatique et en automatique (Inria) et à l'université Pierre-et-Marie-Curie, a conçu pour l'occasion une messagerie sécurisée par

un algorithme de cryptographie post-quantique. Le logiciel a tourné sur un smartphone, un Samsung fonctionnant sous Android. Grâce à une clé de chiffrement ultra-optimisée, les communications ont pu être sécurisées sans ralentir les communications. Une interface spécifique de messagerie avait été conçue par la start-up Wasssa. PolSys, qui cherche à valoriser sa technologie, est en phase de recherche de fonds d'investissement afin éventuellement de créer une start-up. ■