Figure 1 : La câblier «Sophie Germain» en mer.

Un nouveau navire câblier pour Orange-Marine

Le 22 septembre dernier, à Toulon, Orange a inauguré son nouveau navire câblier, baptisé du nom de « Sophie Germain » mathématicienne française (1776-1831) d'une époque où rares étaient les femmes qui pouvaient accéder à la culture scientifique. Elle s'est illustrée dans la théorie des nombres et dans celle des vibrations des surfaces élastiques et a été la première femme à recevoir, en 1816, le grand prix de mathématiques de l'Académie des sciences.

Ce nouveau navire câblier remplace le « Raymond-Croze » lancé en 1983 qui va être désarmé. Il est spécialisé dans des missions de maintenance de câbles sous-marins en Méditerranée, en mer Rouge et en mer Noire. Il complète la flotte de sept navires d'Orange Marine qui représente 15 % de la flotte de câbliers mondiale. Innovation et pari sur l'avenir, il est équipé pour traiter les pannes aussi bien des câbles sous-marins de télécommunications que ceux de transport d'électricité, notamment ceux reliant les éoliennes en mer aux réseaux électriques ; il n'est pas destiné à poser de nouveaux câbles et ne dispose pas de moyens de pose à grande échelle. Pour mener à bien sa mission, il emporte à son bord un robot sous-marin de dernière génération, le ROV [1] Alpha, conçu pour effectuer des travaux sous-marins jusqu'à une profondeur de 3000 m.

1 ROV : *Remotely Operated Vehicle* (véhicule commandé à distance)

Figure 2 : Le ROV Alpha - Source : Orange Marine.

Cet engin d'un poids de 12 tonnes est piloté et alimenté à partir du navire et se meut sur le fond marin grâce à ses chenilles : il est doté de caméras (jusqu'à 6) et d'une caméra à haute définition, d'altimètre, de sonar, de fonctions de détection des métaux, et de moyens mécaniques permettant d'accéder aux câbles même enfouis. Il est capable de creuser une tranchée sous-marine d'une profondeur pouvant atteindre trois mètres d'inspecter un câble, de le sectionner et éventuellement d'enfouir une nouvelle section de câble remplaçant la section défectueuse. Le ROV Alpha a été conçu et fabriqué en France par une filiale d'Orange Marine.

Dans la conception du navire, d'une longueur de 100 mètres, une attention particulière a été portée à la limitation de son impact environnemental : utilisation d'un fuel à faible taux de soufre (< 0,1 %), à quai alimentation électrique extérieure, fournie notamment par des panneaux solaires lorsqu'il est à sa base d'attache, La Seyne. Sa propulsion est assurée par des moteurs électriques alimentés par quatre ensembles de générateurs et des batteries : en fonction de la puissance nécessaire à la phase de la mission en cours un ou plusieurs ensembles de générateurs peuvent être utilisés, limitant ainsi le carburant consommé aux besoins effectifs. Les eaux usées traitées peuvent être stockées pendant 7 jours. Son empreinte environnementale est réduite par rapport aux câbliers classiques : -20 % en termes d'émission de CO_2 et -82 % en termes d'émission d'oxyde d'azote selon Orange.

Le personnel embarqué peut atteindre 76 personnes

Avec la mise en service de ce nouveau navire, Orange poursuit sa contribution au maintien en service permanent des câbles sous-marins qui constituent une infrastructure essentielle aux réseaux de communication et d'énergie et pourraient dans la période de tensions internationales actuelles devenir des cibles d'actions malveillantes. La France, avec Orange Marine et Alcatel Submarine Networks qui dispose aussi d'une flotte de sept navires câbliers est un acteur essentiel dans la construction et la maintenance des réseaux sous-marins. ■ **PC**

Situation énergétique de l'Ukraine à fin octobre 2023

En dépit de la situation exceptionnelle due à la guerre, le système électrique ukrainien continue de fonctionner.

Malgré la situation exceptionnelle due aux combats, et en dépit des destructions d'infrastructures de transport et de distribution d'électricité, certes compensées par une réactivité remarquable des équipes des opérateurs pour les réparer voire reconstruire (figure 1), le système électrique ukrainien continue de fonctionner dans un contexte marqué par une baisse significative de la consommation par rapport à l'avant-guerre, du fait des migrations des populations qui ont quitté certaines zones, et de la chute de l'activité économique.

Figure 1 : Lignards de la compagnie DTEK réparant une ligne 150 kV après le bombardement de Kherson en août 2023 (source DTEK).

Depuis le début de la guerre en Ukraine, selon les données du Haut-Commissariat des Nations unies pour les réfugiés (HCR), plus de 7,2 millions d'Ukrainiens ont quitté le pays, soit une baisse de la population de l'ordre de 18 %.

Voici quelques chiffres du mois d'octobre 2023 pour illustrer cette situation :

- La consommation électrique moyenne journalière a été à peu près réduite d'un tiers, avec pour le mois d'octobre une puissance appelée horaire moyenne qui est passée de 17- 18 à 11-12 GW. En parallèle, la pointe hivernale en moyenne journalière horaire est passée de 20 à 12-13 GW.

- Face à cette consommation, la production se répartit ainsi en octobre 2023 (leur localisation est illustrée en figure 2) :
• 60 à 65 % de nucléaire.
• 15 à 25 % de thermique à flamme, principalement du charbon.
• 10 à 15 % d'hydraulique (en baisse depuis la destruction du barrage de Kakhovka).
• 2 à 5 % pour les turbines à gaz
• Le reste en renouvelable solaire et éolien (moins de 10 %).

Depuis la connexion au système électrique européen voilà plus d'un an, des échanges commerciaux sont possibles, ainsi que des contrats de secours avec les gestionnaires de réseau interconnectés. Mais du fait de la capacité du système ukrainien à couvrir ses besoins et même à être excédentaire avec des coûts de production ●●●

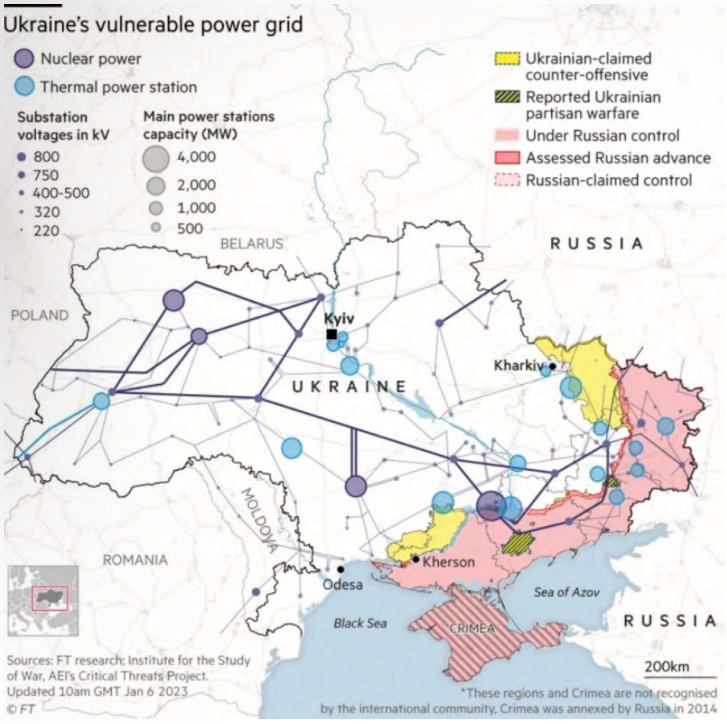

Figure 2 : Localisation des centrales de production électrique en Ukraine (source FT).

très compétitifs par rapport à ceux de ses voisins, les importations ont été très peu utilisées.

Après la récente levée par le ministère ukrainien d'une mesure de limitation des exports prise par précaution, les exportations se sont développées, notamment durant l'été vers la Slovaquie et la Moldavie, avec un solde import/export journalier principalement orienté à l'export, et variant selon les jours de 1 GWh d'import à 4 GWh d'export sur la semaine du 16 au 23 octobre 2023 par exemple.

La préparation de l'arrivée de l'hiver et de la saison de chauffe est en cours. Compte tenu des réparations des centrales endommagées qui ont eu lieu cet été, et celles escomptées d'ici à l'arrivée de l'hiver, l'Ukraine aura besoin d'importations à hauteur de 2 GW pour passer les pointes, avec une puissance consommée qui pourrait atteindre 16,7 GW alors que le total disponible en production serait de 13,8 à 14,7 GW selon l'avancée des réparations restantes jusqu'en décembre. Les stocks de charbon seraient quant à eux suffisants. ■ **HL**

Etape importante de la normalisation de la cryptographie quantique

Les organismes de normalisation comme le NIST aux Etats Unis ou de sécurité comme l'ANSSI en France se préoccupent de définir de nouveaux algorithmes résistants aux futurs ordinateurs quantiques.

La menace de l'ordinateur quantique sur les systèmes de cryptographie

La cryptographie post-quantique contrairement à la présence du terme quantique dans son intitulé n'est pas une cryptographie quantique améliorée mais une réponse à l'article de Peter Shor en 1994 qui dévoilait un algorithme quantique capable de factoriser un entier très grand dans un temps polynomial. A partir de la publication de cet article les spécialistes des systèmes de cryptographie basés sur le problème de la factorisation d'entiers, problème mathématique réputé difficile, ont entrepris des recherches pour échapper à cette faille de sécurité.

Le développement et plus encore la production d'ordinateurs quantiques ayant la capacité en nombre de bits quantiques (qubits) de factoriser les systèmes de cryptographie n'était pas encore possible au début des années 2000. Cependant les progrès rapides des ordinateurs quantiques dans la décennie 2010 laissaient penser que le risque de casser les systèmes de cryptographie employés dans les réseaux publics devenait majeur à des échéances de moins en moins lointaines (voir par exemple la figure 1). Le domaine de recherche suscité pour répondre à cette faille de sécurité a été appelé cryptographie post-quantique. Avec pour ambition de renforcer les systèmes qui pouvaient être mis en difficulté par un ordinateur quantique. Les organismes de normalisation comme le NIST (*National Institut of Standards and Technology*) des Etats-Unis ou de sécurité comme l'ANSSI (Agence nationale de la sécurité des systèmes d'information) en France se sont donc préoccupés de définir de nouveaux algorithmes résistant aux futurs ordinateurs quantiques

Les standards NIST

Le NIST a organisé en 2016 un concours international pour la standardisation des algorithmes cryptographiques post quantiques. Dans le cadre de ce concours, le NIST a publié le 5 juillet dernier une liste qui comprend les quatre premiers algorithmes sélectionnés à partir de sept finalistes, un algorithme d'établissement de clé nommé CRYSTALS-Kyber et trois algorithmes de signature appelés CRYSTALS-Dilithium, FALCON et SPHINCS+. Les trois premiers de ces algorithmes sont fondés sur les réseaux euclidiens structurés ; le dernier, SPHINCS+, est fondé sur des constructions en arbres de hachage. Les normes fédérales américaines devraient suivre ces recommandations mais il est clair que ces annonces sont à portée mondiale. C'est la conséquence du caractère international de la compétition entre les acteurs de la communauté de recherche en cryptographie mais aussi parce qu'il est habituel que les normes américaines s'imposent comme des standards industriels mondiaux. En complément aux choix des quatre

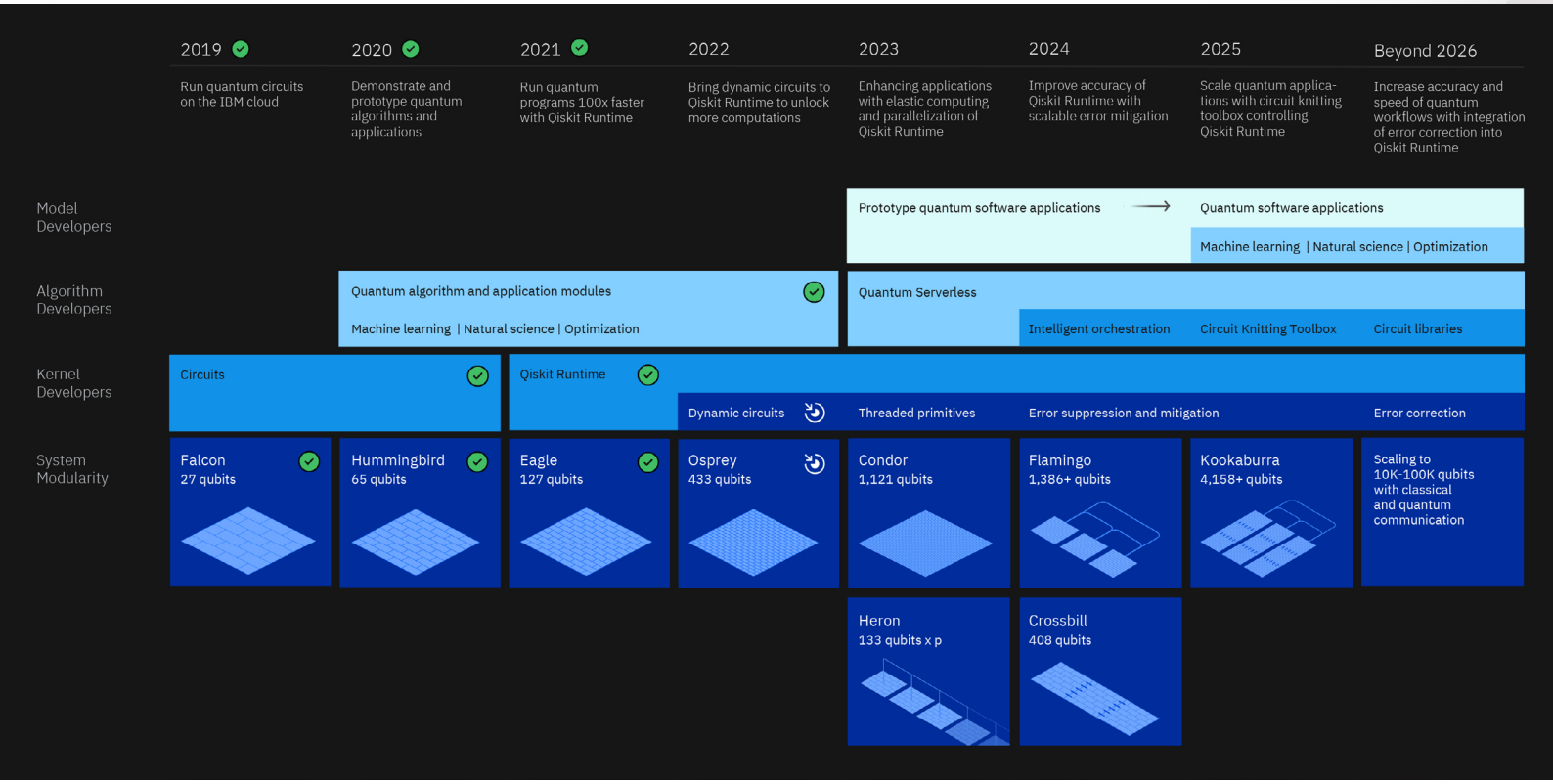

Figure 1 : Feuille de route des recherches IBM montrant l'augmentation du nombre de qubits par années jusqu'au-delà de 2026. (Source IBM).

algorithmes, une campagne d'étude de standardisation est prévue pour quatre autres algorithmes dont trois sont fondés sur des correcteurs d'erreur et le quatrième sur les graphes de courbes elliptiques. Il est probable que ces derniers pourraient rejoindre le processus de standardisations des quatre algorithmes précités. L'objectif final du NIST est de pouvoir standardiser un grand éventail d'algorithmes afin de couvrir une majorité de cas d'application à l'horizon 2024. Les quatre algorithmes CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON et SPHINCS+ peuvent être considérés comme des choix à envisager dans la majorité des cas lors de la sélection d'algorithmes post-quantiques pour la conception de produits de sécurité.

La stratégie quantique française de l'ANSSI

L'organisme français ANSSI s'est montré satisfait du choix effectué par le NIST et les algorithmes choisis semblent offrir des perspectives raisonnables quant à leur sécurité à long terme. Au niveau national, des stratégies ont été mises en place, Emmanuel Macron à la fin de l'année 2022 avait, dans un tweet, révélé le premier envoi d'un télégramme diplomatique sécurisé grâce à la cryptographie post-quantique. La doctrine française en ce qui concerne les algorithmes post-quantiques, présentée dans l'avis scientifique et technique de janvier 2022, n'est pas modifiée par l'annonce du NIST. Même si ces algorithmes sont prometteurs, l'ANSSI ne recommande en aucun cas le remplacement direct des algorithmes actuels par ces nouveaux futurs standards. Mais à l'inverse, l'agence avait annoncé qu'à partir de 2020 elle ne labelliserait plus les technologies de chiffrement qui ne résisteraient pas aux ordinateurs quantiques.

Dans les années qui viennent, ces algorithmes post-quantiques devront encore être utilisés dans un mode hybride, c'est à dire combinés avec un algorithme à clé publique pré-quantique reconnu et éprouvé. la sélection opérée par le NIST ne doit pas être comprise comme une liste fermée d'algorithmes post-quantiques utilisables. En effet, certains algorithmes non retenus semblent disposer d'une sécurité à long terme au moins équivalente à celle des algorithmes sélectionnés. Ainsi l'ANSSI souhaite continuer à encourager la recherche et la R&D en cryptographie post-quantique, soit qu'il s'agisse de l'analyse de la difficulté des problèmes mathématiques sous-jacents, soit de l'intégration des algorithmes post-quantiques dans des protocoles hybrides de communication et de l'analyse de sécurité. Les quatre algorithmes sélectionnés et les quatre algorithmes retenus pour le prolongement de la campagne de standardisation sont le résultat de coopérations internationales mais la liste de leurs co-auteurs et leurs affiliations illustrent l'extraordinaire vitalité de la recherche française et de la recherche européenne en cryptographie. ■ **ML**