Innovation de rupture et cybersécurité

William LECAT
Directeur de Programme
Grand Défi automatisation de la cybersécurité
Secrétariat Général pour l'Investissement

La rupture

Il est important de bien distinguer les notions de rupture technologique et d'innovation de rupture. La première nous offre de nouvelles possibilités, alors que la deuxième amène de nouvelles applications. En effet, l'innovation de rupture au sens où on l'entend en général est centrée sur la modification des usages. Néanmoins, le lien entre les deux reste étroit et bidirectionnel dans la mesure où de nouveaux usages stimulent des ruptures technologiques pour mieux y répondre et où les ruptures technologiques ouvrent de nouvelles possibilités pour l'innovation d'usage.

On retrouve principalement trois types d'innovation de rupture. Celui qui vient le plus facilement à l'esprit concerne la « rupture de marché ». Il s'agit à la fois d'un nouvel usage et d'un nouveau marché. C'est par exemple le cas d'AirBnB qui amène un nouvel usage de location de logements de particuliers dans le cadre d'une plateforme en ligne grand public. Le deuxième type correspond à la « rupture de sens ». Ici, un nouvel usage est poussé sur un marché existant. L'illustration typique est l'apparition de l'iPhone qui révolutionne l'usage du téléphone portable. Enfin, le dernier type correspond à une « rupture par le bas » rendant accessible au plus grand nombre un usage existant (par exemple, la Ford T ou les vols low cost).

Par définition, une technologie de rupture est (le plus souvent) une technologie naissante. Il arrive donc fréquemment qu'elle sous-performe par rapport à l'existant, à sa création. Ce n'est qu'avec une certaine maturité que cette nouveauté pourra supplanter les technologies devenues obsolètes. Ce processus peut parfois donner l'impression qu'anticiper ce type de rupture est plus aisé en identifiant des technologies prometteuses parmi celles en cours de maturation. Il n'en reste pas moins que l'anticipation de la rupture elle-même, c'est-à-dire de la création et non de la maturation de la technologie, est très ardue, voire impossible.

De même, l'innovation de rupture peut troubler par son apparente simplicité à la fois du nouvel usage et, souvent même plus, de la technologie sous-jacente. Trop souvent, les innovations de rupture sont considérées comme ne reposant pas sur des ruptures technologiques, or c'est assez fréquemment le cas. Si la coïncidence (voire la précédence) temporelle de la rupture d'usage avec la rupture technologique est assez rare, il n'en reste pas moins que, pour reprendre les exemples précédents, AirBnB a été rendu possible par la démocratisation d'Internet à la suite de l'arrivée de l'ADSL puis de la 3G et de la 4G ; que l'iPhone s'est appuyé à sa création sur les technologies tactiles et sur la 3G, etc.

Déterminer lequel des deux, de l'usage et de la technologie, est le premier correspond souvent au problème de l'œuf et de la poule, les deux étant parties prenantes dans un cycle. En effet, les nouvelles technologies en maturation amènent de nouvelles possibilités engendrant de nouveaux

usages, appelant de nouvelles technologies. La richesse de l'innovation d'un domaine est donc particulièrement dépendante de la vitesse de révolution de ce cycle et de son intrication avec les cycles des domaines connexes.

En réalité, l'absence de ruptures technologiques rend l'innovation de rupture plus difficile. De plus, la maîtrise de ces technologies de rupture est un prérequis minimal pour pouvoir les appliquer.

Il n'en reste pas moins que l'arrivée d'une rupture technologique est très rarement couplée à une innovation de rupture. Il semble que pour impulser de nouveaux usages, ces technologies doivent être en mesure d'atteindre certains niveaux de maturité. C'est d'ailleurs logique puisque les innovations de rupture sont le plus souvent des innovations d'usage, elles s'appuient donc sur des usages. Il est donc fondamental que ces technologies sous-jacentes soient prêtes pour une application industrialisée.

La cybersécurité

Dans ce contexte, le cas de la cybersécurité est très spécifique. En effet, la cybersécurité existe pour les besoins d'un autre marché : le numérique. Ce dernier est bien souvent un catalyseur vis-à-vis d'autres domaines (industrie, médical, transport, etc.). Le dynamisme de la cybersécurité est ainsi largement favorisé par ses multiples applications, chaque nouveauté dans un domaine d'application pouvant stimuler une innovation en cybersécurité. Cette effervescence est renforcée par la rapide évolution des technologies (parfois de ruptures) et leurs applications galopantes à tous les domaines ouvrant ainsi la porte à de nombreuses innovations de rupture. Tous ces éléments contribuent à expliquer les évolutions rapides sur des cycles très courts dans ce secteur.

La cybersécurité est donc naturellement exposée à de nombreuses ruptures technologiques ou d'usage dans le secteur en lui-même (par exemple, l'application de l'intelligence artificielle pour la détection de menaces), mais aussi dans ses domaines d'application (objets connectés, 5G, etc.). Il y a ainsi une distinction à faire entre de nouveaux usages de cybersécurité et la cybersécurité des nouveaux usages. Ce dernier aspect est souvent considéré comme une menace ou un problème du point de vue de la sécurité. En effet, les ruptures d'usage arrivant de plus en plus vite et se diffusant tout aussi rapidement, l'adaptation de la sécurité pour les prendre en compte est souvent en retard et dans tous les cas, confinée à une position réactive. La réponse à ce problème a été trouvée depuis longtemps déjà : il faut être sécurisé « by design » et non pas a posteriori. Il est d'ailleurs essentiel que la cybersécurité ne soit pas un frein à ces nouveaux usages pour faciliter son adoption rapide et la plus large possible. C'est bien sûr ce vers quoi il faut tendre, grâce aux prises de conscience des utilisateurs et des fournisseurs, et par la réglementation dans certains cas. Néanmoins la route est encore longue. Malgré tout, même dans une configuration idéale, certaines problématiques subsistent dans la mesure où l'impact et l'évolution de ces nouveaux usages sont difficilement prédictibles et dès lors que la sécurité peut être affectée de manière inattendue.

À l'opposé, du point de vue de l'innovation, les évolutions constantes dans les domaines d'application de la cybersécurité représentent des opportunités. Innover constamment est donc nécessaire que ce soit en adressant de nouveaux usages (nécessitant parfois des ruptures technologiques en cybersécurité) ou en proposant des ruptures (d'usage) dans la manière d'approcher la sécurité. L'innovation est d'autant plus favorisée par la forte proportion de solutions logicielles pouvant être apportées aux problématiques de cybersécurité. Le développement logiciel présentant moins de barrières à l'entrée que d'autres domaines (nécessitant de grosses infrastructures par exemple), de nouveaux acteurs apparaissent en permanence.

Face à cette marche forcée de l'innovation, les acteurs économiques fournisseurs de cybersécurité sont tiraillés entre une recherche de stabilité, la conquête de nouveaux marchés et la concurrence toujours plus diverse. S'il est bien clair pour de tels acteurs qu'une innovation permanente est un prérequis, les démarches d'anticipation restent variées. Or, il apparaît qu'anticiper de nouveaux besoins correspond plus à être proactif sur les innovations incrémentales dans les domaines d'applications alors que l'arrivée de nouveaux usages (innovation de rupture) n'est que rarement anticipée (sinon, la rupture serait moindre, les usages pouvant s'adapter progressivement) à part par ceux qui les poussent, et encore.

Grand Défi cyber

Les cycles courts et les évolutions rapides de la cybersécurité imposent une maturation rapide des technologies afin de resserrer le lien entre les usages et les technologies. C'est exactement dans ce cadre que s'inscrit le Grand Défi cyber, l'objectif étant de financer des technologies pouvant faire émerger une rupture tout en poussant de nouveaux usages. Ainsi, pour tous les projets soutenus, on cherchera à établir un partenariat avec un industriel qui amènera sa problématique et qui pourra bénéficier des nouvelles approches permises par les technologies et les produits développés. L'idée est de pouvoir procéder à des expérimentations en boucles courtes pendant le développement pour arriver le plus rapidement possible à un produit utilisable, basé sur de nouvelles technologies.

Le découpage de la sélection et de la réalisation des projets reflète cette démarche. En effet, une première phase du Grand Défi devrait débuter la semaine prochaine (avec l'ouverture des candidatures) et s'achèvera de manière simultanée pour tous les projets en janvier 2022. On prévoit donc entre 12 et 15 mois de réalisation. À l'issue, une seconde sélection aura lieu pour accélérer les projets les plus prometteurs, qui auront amené des ruptures technologiques et d'usage, sur une période de 11 mois jusqu'à fin 2022 constituant la seconde phase.

Sur ces deux phases, environ 25 millions d'euros provenant du Grand Défi, principalement sous forme de subvention à un taux pouvant aller jusqu'à 50 %, seront dédiés au financement des projets pour lever des verrous technologiques et développer des technologies de rupture. Il s'agira donc d'un co-investissement (public/privé) d'au moins 50 millions d'euros.

Les projets sélectionnés seront centrés sur les trois axes verticaux de la feuille de route du Grand Défi : l'impact des nouveaux usages sur les réseaux, les objets connectés et la protection des petites structures.

Cette démarche devra préfigurer des initiatives de plus grande ampleur pouvant prendre le relai et permettant à la France de devenir un leader mondial dans le domaine de la cybersécurité.