

OBSERVATOIRE DU MONDE CYBERNÉTIQUE



Lettre n°58-Janvier 2017-disponible sur omc.ceis.eu



« According to our latest evaluations, there was a monthly average of 500 threatening cyber attacks last year against NATO infrastructure that required intensive intervention from our experts. [...] Most of these attacks did not stem from private individuals but were sponsored by national institutions of other countries. [...] I am extremely concerned about this development. Cyber defense will play an important role at the next NATO summit, and we'll need to step up our efforts in this area.», Jens Stoltenberg, secrétaire général de l'OTAN.

TABLE DES MATIERES

• LE RAPPORT A L'INDEPENDANCE NUMERIQUE EN INDE.....	2
Le numérique en Inde : une richesse tournée vers l'international.....	2
La fracture numérique	4
Une réelle recherche d'indépendance numérique ?.....	6
• HACKATHON : COMMENT PEUVENT-ILS CONTRIBUER A L'INNOVATION EN MATIERE DE CYBERSECURITE ?.....	9
Le hackathon-type	9
Incubation et accélération.....	10
Quelques exemples de hackathons centrés sur la « cybersécurité ».....	11
Bonnes pratiques.....	12



LE RAPPORT A L'INDEPENDANCE NUMERIQUE EN INDE

Connue pour être le carrefour mondial du développement logiciel, l'Inde fait relativement peu parler d'elle en matière de cybersécurité. Au moment des révélations Snowden, l'Inde ne possédait pas de politique officielle en matière de cybersécurité. C'est donc en réponse à celles-ci que le gouvernement a dévoilé son premier plan, le *National Cyber Security Policy 2013*, le 2 juillet de la même année.

Au niveau international, le pays a rejoint plusieurs mécanismes de coopérations dans le domaine cyber en 2016, avec des partenaires occidentaux (l'US-India Cyber Relationship Framework, le partenariat avec l'Union Européenne et la Malaisie¹), mais également avec les membres des BRICS² et notamment la Russie (concrétisé en marge du sommet des BRICS à Goa en octobre³).

Face aux initiatives d'indépendance et de souveraineté numérique de ses partenaires des BRICS, quel est, dans le contexte qui est le sien, le rapport de l'Inde à ces notions ?

Le numérique en Inde : une richesse tournée vers l'international

Le secteur logiciel global en Inde

La révolution IT aux Etats-Unis dans les années 80-90 a grandement tiré parti de la main d'œuvre indienne. Débutant sous la forme d'une immigration d'ingénieurs et de techniciens en quête d'opportunités, la forte croissance de ce secteur a donné lieu à l'émergence d'entreprises tournées vers le développement de logiciels à destination de l'étranger⁴. Celles-ci, qui ont pu compter sur un vaste bassin de ressources humaines parlant anglais, comprennent notamment TCS, WIPRO ou encore Infosys.

Au niveau mondial, l'Inde fait figure de centre incontournable dans le domaine du numérique. L'industrie du logiciel indien exporte au total pour 110 milliards de dollars, et possède 60% des parts de marché d'externalisation au niveau mondial⁵. Sur les 10 premières entreprises de service logiciel au niveau mondial, 5 sont indiennes, et au sein de ces 10 entreprises, 70% des salariés sont indiens. Ces exportations dominent l'industrie du logiciel et la rendent très dépendante de la demande extérieure, puisqu'elles constituent 77% de ses revenus.

Ce secteur est ainsi très dépendant de la conjoncture économique et politique mondiale. Les marchés se sont contractés à la suite de la crise économique de 2008 et ne connaissent plus la croissance à deux chiffres d'antan. Le risque du développement de mesures protectionnistes aux Etats-Unis, du fait de l'arrivée au

¹ <https://securityintelligence.com/as-india-gears-up-for-cybersecurity-challenges-threats-are-multiplying/>

² http://news.xinhuanet.com/english/2016-09/15/c_135689868.htm

³ <http://www.orfonline.org/expert-speaks/india-and-russia-cyber-agreement/>

⁴ <http://www.indiastudychannel.com/resources/151102-History-Information-Technology-India.aspx>

⁵ <http://www.outlookindia.com/website/story/the-grim-future-of-it-companies/297316>

pouvoir de Donald Trump, effraie particulièrement ces entreprises⁶, alors même que leur modèle économique se trouve également menacé par le développement de l'automatisation et du Cloud Computing⁷.

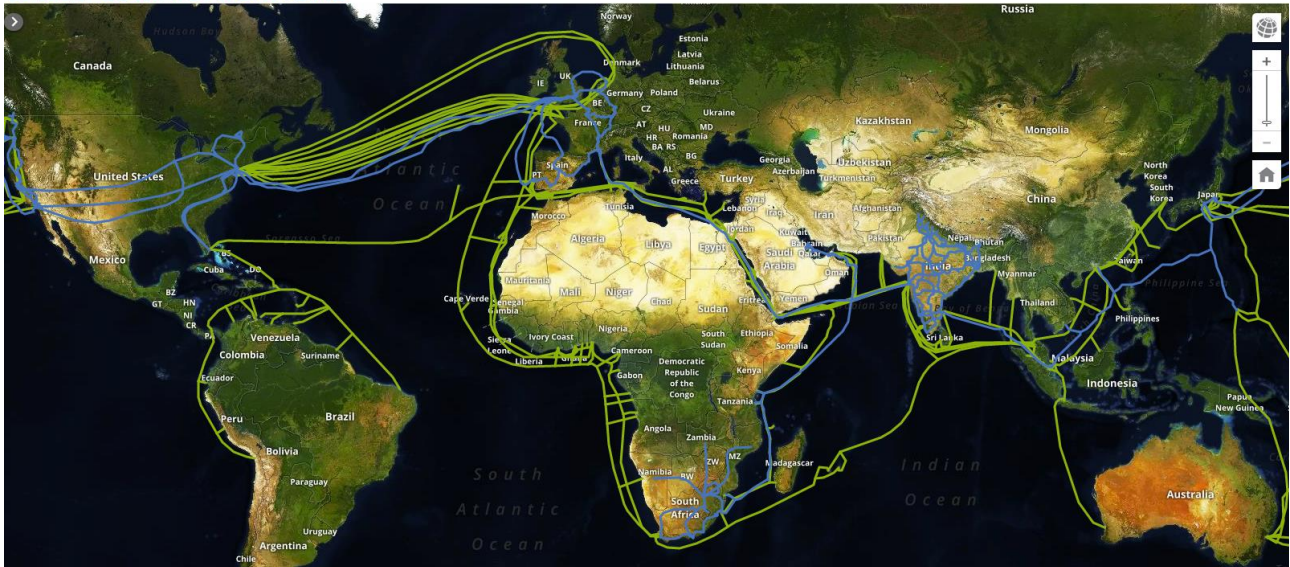
La question des réseaux de communication

L'industrie des télécoms en Inde a connu une libéralisation à marche forcée au cours des années 90, qui a donné naissance à plusieurs champions d'envergure internationale, tels que Tata, Airtel ou encore Reliance. Ceux-ci se partagent ce qui est devenu le deuxième marché mondial de téléphonie (fixe et mobile) et d'Internet.

En matière d'infrastructures réseaux, c'est le groupe indien Tata qui s'est le plus développé à l'international : il possède en effet un réseau de câbles sous-marins qui fait transiter près d'un quart du trafic Internet mondial. Tata Communications, sa filiale télécoms, dispose d'un réseau international de 700 000 km, dont 500 000 km reposent au fond des océans. Cette richesse d'infrastructure lui confère un avantage concurrentiel important face aux géants des télécoms : le propriétaire des câbles sous-marins possède en effet également le premier point de contact où la latence est la meilleure et dont l'accès se monnaie au prix fort. Le groupe, après avoir connecté l'Inde, est rapidement parti à l'international relier les continents entre eux, si bien que les trois quarts de son chiffre d'affaires (3.1 milliards de dollars) sont réalisés à l'international. Si la société a récemment investi 1.2 milliards de dollars dans ses infrastructures, elle a cependant décidé de ralentir ses investissements : les géants du web, dont les besoins ne cessent de grandir, ont en effet commencé à construire leurs propres infrastructures. Face à cette nouvelle donne, le groupe indien choisit aujourd'hui de se concentrer sur les offres de services aux entreprises, profitant de la richesse du pays en ressources humaines dans le secteur de l'informatique.

⁶ <http://economictimes.indiatimes.com/tech/ites/why-trump-buy-american-hire-american-campaign-will-hit-indian-it-companies-hard/articleshow/56714370.cms>

⁷ <http://www.ft.com/cms/s/0/f5dd86a2-8b8d-11de-9f50-00144feabdc0.html>



Réseau de câbles sous-marins du groupe Tata. En bleu, les câbles appartenant à la compagnie, en vert, les câbles partagés avec d'autres opérateurs
Source : Tata Communications

La fracture numérique

Malgré la forte présence des entreprises indiennes dans les secteurs des télécoms et de l'informatique, l'accès au numérique est très inégal selon les régions. Le taux de pénétration d'Internet en Inde se situe aux alentours de 35% en 2016, ce qui correspond à 462 millions d'utilisateurs⁸. Le fait que les deux tiers de la population soit rurale explique en grande partie ce « faible » taux d'usage. A cela s'ajoutent les problèmes de la langue et du taux d'alphabétisation. Ce dernier s'élevait à 74% en 2011⁹, et l'anglais, qui constitue la quasi-totalité de l'Internet indien, est peu parlé en dehors des villes.

Le 1^{er} juillet 2015, le Premier Ministre Narendra Modi a lancé la campagne **Digital India**. Celle-ci a pour objectif le développement :

- De l'infrastructure digitale ;
- De la maîtrise du numérique, ou « Digital Literacy¹⁰ ».
- De l'e-gouvernance et la digitalisation des services à l'utilisateur.

Le développement de l'infrastructure digitale vise tout d'abord à fournir de la connectivité au plus grand nombre, notamment dans les campagnes. BBNL, le fonds commun de créances (en anglais SPV) créé par le ministère des télécoms indien, avait ainsi choisi United Telecoms Limited pour connecter 250 000 villages par la fibre d'ici à 2017. Ce choix a été effectué notamment sur la base de son offre financière, inférieure de 80% à celles de ses concurrents. Au 10 janvier 2017, seuls 27,5% des collectivités ciblées ont été connectées

⁸ <http://www.internetlivestats.com/internet-users/india/>

⁹ <http://www.census2011.co.in/literacy.php>

¹⁰ https://en.wikipedia.org/wiki/Digital_literacy

d'après le *dashboard* de performances du gouvernement¹¹. Ce besoin de connectivité comprend également les réseaux mobiles, puisque plus de 55 000 villages n'avait pas de couverture mobile en 2015.

La maîtrise du numérique correspond à la connaissance et aux compétences liées à l'utilisation connectée des dispositifs digitaux tels que les ordinateurs, tablettes et autres smartphones. Cela comprend la capacité de participer à des communautés en ligne tout en adhérant aux protocoles comportementaux attendus par celles-ci (sens de l'esprit critique, respect des normes éthiques, etc.), ou encore à savoir utiliser un moteur de recherche. La notion de Digital Literacy peut trouver son origine dans la Media Literacy au Royaume-Uni et aux Etats-Unis, qui avaient respectivement pour objectifs de lutter contre la propagande dans les années 30 et contre les excès de la publicité dans les années 60. Il s'agissait d'apprendre aux individus à identifier les biais au sein des messages auxquels ils étaient confrontés.

Aujourd'hui, la maîtrise du numérique fait également partie des 9 éléments centraux de la citoyenneté numérique.

Enfin, un dernier axe de développement vise à créer de nouveaux services à la personne. Ces services concernent, entre autres, le développement de l'hôpital numérique, la mise en place d'un système de signature électronique multifacteur *Aadhaar* (incluant la biométrie¹²), la création d'un Cloud citoyen (*DigiLocker*), ou encore d'un système de pointage pour les employés de l'administration (*attendance.gov.in*). Il s'agit de réduire les coûts (notamment à travers l'élimination du papier) et d'améliorer l'efficacité de l'administration. Enfin, et de façon plus anecdotique, le plan prévoit de faire participer le citoyen à la gouvernance, avec la mise en place d'une plateforme de type boîte à idée (*MyGov.in*).

Ce troisième axe du plan gouvernemental dépend bien entendu de l'effectivité du développement de l'infrastructure numérique du pays et de la maîtrise de cet espace par la population. Digital India constitue également une opportunité pour le gouvernement de soutenir l'industrie du numérique en Inde, qui représente aujourd'hui 5% des emplois dans le pays. Mais cela n'exclut pas pour autant les GAFAM, qui se sont montrés évidemment très favorables au projet Digital India, y voyant une opportunité d'accroître leur marché.

Parallèlement au programme Digital India, l'Inde investit massivement dans le développement de Smart Cities. Le programme Smart Cities Mission, démarré en juin 2015, prévoit ainsi le développement d'une centaine de villes « smart », soit un investissement de 7 milliards de dollars¹³.

¹¹ <https://web.archive.org/web/20170110130531/https://transformingindia.mygov.in/performance-dashboard/>

¹² <http://economictimes.indiatimes.com/news/economy/policy/uidai-registration-for-all-aadhaar-authentication-devices-soon/articleshow/56734738.cms>

¹³ <http://smartcities.gov.in/writereaddata/SmartCityGuidelines.pdf> ; https://en.wikipedia.org/wiki/Smart_Cities_Mission

Une réelle recherche d'indépendance numérique ?

Le matériel

Alors que la demande de matériel électronique totale du pays pourrait atteindre 400 milliards d'ici à 2020, la production domestique estimée ne dépasserait 104 milliards. L'import de biens électroniques dépasserait ainsi celui de pétrole¹⁴.

Le niveau d'importation de produits électroniques du pays s'élevait à 36 milliards en 2015¹⁵, dont près de la moitié est constituée par les téléphones. L'Inde devrait constituer le deuxième marché mondial des smartphones, devant les Etats-Unis, et pour cette raison, les entreprises étrangères ont commencé à investir dans la création d'usines dans le pays¹⁶. Cela a notamment été facilité par le programme gouvernemental Make in India lancé en septembre 2014, qui a largement ouvert l'investissement étranger direct dans de nombreux secteurs de l'économie indienne, dont l'électronique. Ce plan a permis à l'Inde de devenir la première destination des investissements étrangers direct, devant la Chine et les Etats-Unis.

Le développement d'une industrie locale de matériel informatique reste cependant pénalisé par la faiblesse des infrastructures de transport. Le manque d'investissements dans ce domaine diminue l'attrait de l'Inde auprès des investisseurs étrangers : les coûts combinés de la logistique dans le pays atteindraient en effet 14% du PIB, le double de la part habituelle pour un pays émergent¹⁷.

Et si le gouvernement a favorisé l'industrie locale en imposant une taxe de 12,5% sur les importations de tablettes et de smartphones, celle-ci ne s'étend pas aux équipements réseaux (switches, routeurs, etc.) : le gouvernement indien semble encore relativement éloigné du concept de souveraineté numérique cher à son voisin chinois.

Alors que le gouvernement indien a demandé en octobre 2015 qu'au moins la moitié des ordinateurs achetés par les agences gouvernementales proviennent du marché domestique, la volonté politique réelle semble faible. Le gouvernement a effectivement opté pour une définition large de ce qui doit être considéré comme constituant l'industrie locale : seuls 30% des composants de l'ordinateur doivent être fabriqués en Inde, les composants qui y sont assemblés sont considérés comme y étant fabriqués, et ces fameux 30% peuvent correspondre à une simple valeur ajoutée « made in India ».

En 2009, le Centre pour la Recherche Scientifique et Industrielle (CSIR) a proposé au gouvernement la création d'une entreprise destinée à porter le projet de développement d'un microprocesseur national¹⁸. Si des raisons économiques ont été avancées pour justifier ce projet (l'industrie du matériel informatique dépendait alors à 70% des importations), c'est avant tout la sécurité nationale qui était mise en avant dans la proposition.

¹⁴ <http://economictimes.indiatimes.com/industry/cons-products/electronics/electronics-import-may-rise-to-40-billion-in-fy16-due-to-smartphone-led-surge/articleshow/49460156.cms>

¹⁵ <http://www.worldstopexports.com/indias-top-10-imports/>

Ces chiffres ne prennent pas en compte le matériel embarqué (automobile, matériel médical, etc.).

¹⁶ <http://www.livemint.com/Industry/14DELtag6kPOIM75ynD5RK/Has-Indias-electronic-manufacturing-turned-a-corner.html>

¹⁷ http://ebtc.eu/pdf/130108_MAS_Overview-of-the-demand-in-the-Indian-transport-and-logistics-industry.pdf

¹⁸ <http://www.livemint.com/Home-Page/P8hJk0uMYmajN0tFph692K/Why-a-madeinIndia-chip-remains-chimeric.html>

La crainte reposait déjà à l'époque sur le risque de *backdoor* dans les produits étrangers, notamment pour les secteurs de l'énergie atomique, de l'espace et pour les réseaux militaires. Le document du gouvernement mentionnait explicitement des réseaux de hackers chinois s'attaquant à des installations sensibles tels que le quartier général du Dalai Lama ou des réseaux télécoms au Royaume-Uni. Ce projet, qui aurait vu le développement d'une puce basée sur l'architecture open-source SPARC, n'a finalement pas reçu la validation – et l'investissement initial – du gouvernement, et n'a donc jamais vu le jour.

Les systèmes d'exploitation

Le National Resource Centre for Free/open Source Software (NRCFOSS) est une organisation créée et financée par le Ministry of Communication and Information Technology en 2005. Celui-ci a développé avec le Centre for Development of Advanced Computing (CDAC) une distribution de Linux basée sur Debian appelée BOSS¹⁹ (Bharat Operating System Solutions), dont la première version date de 2007. Ce système propose l'ensemble des langues officielles indiennes, permettant son utilisation par les non-anglophones, qui représentent 90% de la population.

La Defence Research and Development Organisation (DRDO), l'agence en charge de la recherche et développement pour le Ministère de la Défense indien, a rejoint le projet en 2010 en vue notamment de renforcer la sécurité et de le rendre viable, à la fois pour les forces armées, l'administration et les infrastructures critiques, mais également pour un usage commercial²⁰.

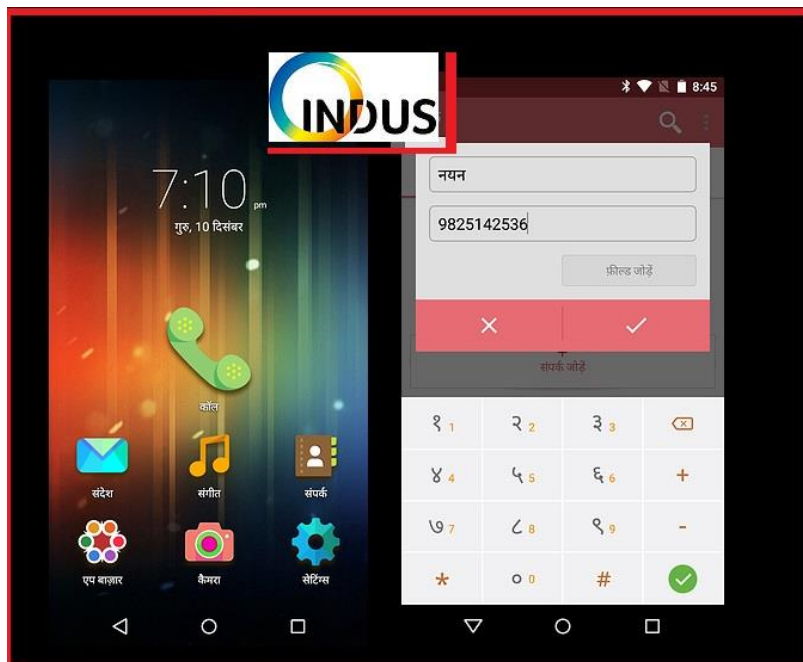
Cependant, le système d'exploitation BOSS n'a pas été suffisamment appuyé pour réaliser une quelconque percée auprès du grand public. Ainsi, on ne retrouve le système indien qu'au sein des institutions gouvernementales et de l'armée, ainsi que la version destinée à l'éducation (eduBOSS) au sein de certaines universités.

Du côté de la mobilité, le système d'exploitation commercial Indus OS a su prendre la seconde place devant iOS, atteignant 7,6% des parts de marché en 2016. Développé en un temps éclair (la société ayant été fondée en 2015), il s'agit à l'heure actuelle principalement d'une surcouche du système Android, dotée d'outils de prédiction et de traduction pour les douze principales langues régionales. Bénéficiant du vivier de développeurs du pays, le marketplace d'Indus OS est celui qui connaît la plus forte croissance du monde²¹.

¹⁹ <https://www.bosslinux.in/>

²⁰ <http://economictimes.indiatimes.com/tech/internet/indian-os-developed-by-drdo-likely-to-be-ready-in-three-years/articleshow/17693044.cms>

²¹ <http://www.newskart.com/indus-a-mobile-operating-system-raises-usd-5-million-series-a-funding-led-by-omidyar-network/>



IndusOS, second système d'exploitation mobile en Inde

L'Inde semble accorder à l'heure actuelle encore relativement peu d'importance à la notion de souveraineté numérique. Au contraire, le pays semble avoir cédé sur la question de la gouvernance Internet, étant revenu sur sa vision multilatérale pour embrasser l'approche multipartite (c'est à dire incluant la société civile et les entreprises privées). Celle-ci, défendue notamment par les Etats-Unis et l'Allemagne, a longtemps été rejetée par l'Inde, par crainte de la domination des entreprises américaines. Un revirement de situation qui n'est peut-être pas étranger au soutien affiché des GAFAM au projet Digital India. Le pays préfère aujourd'hui investir dans la démocratisation de l'accès à Internet et la sensibilisation à ses usages, plutôt que de jouer la carte de la souveraineté numérique. Ceux-ci constituent d'importants différenciateurs de compétitivité, alors que le pays souhaite devenir la nouvelle « usine » mondiale.



HACKATHON : COMMENT PEUVENT-ILS CONTRIBUER A L'INNOVATION EN MATIERE DE CYBERSECURITE ?

Contraction des termes « hack » (« solution rapide et bricolée pour contourner un problème »²²) et marathon, les hackathons sont des compétitions d'innovation se déroulant généralement sur une période assez courte (1 à 2 jours). Qu'ils soient internes ou externes à une organisation, ils partent du principe que l'innovation résulte d'un processus collaboratif qui nécessite de mobiliser un écosystème. Un constat encore plus vrai à l'ère numérique où les cycles technologiques sont très courts et où il s'agit de marier des approches variées, technologiques, *business development*, sciences cognitives etc., pour créer non seulement des technologies innovantes, mais aussi de nouveaux modèles économiques basés sur le service. Né aux États-Unis dans les années 90 au sein de la communauté du logiciel libre, le hackathon fait désormais partie intégrante de la stratégie des entreprises. Et ce, dans de multiples secteurs d'activité : santé, banque et finance, assurance.... Au point que le hackathon contribue désormais à **l'hybridation des technologies et des modèles économiques**, et donc à la transformation numérique de la société.

Si les hackathons constituent une réponse pertinente aux besoins des organisations en matière de transformation numérique, ils sont également particulièrement adaptés à l'innovation en matière de cybersécurité. L'imagination collective qu'ils permettent de structurer et de catalyser est d'abord une réponse à celle, non moins débordante, des cybercriminels ou hackers « non éthiques » qui cherchent les failles des réseaux et systèmes d'information. Par ailleurs, qu'il s'agisse de hackathons dédiés à la cybersécurité ou de défis de cybersécurité intégrés dans des hackathons plus globaux, **ils sont la meilleure façon de développer une approche « by design »**, c'est à dire dès la conception, de la sécurité. Développeurs informatiques, experts en sécurité et juristes peuvent en effet collaborer étroitement pour trouver des solutions innovantes. Ces opérations permettent enfin d'identifier et de valoriser de nouveaux talents ou la ressource humaine est rare.

Le hackathon-type

Le hackathon-type s'articule autour de 4 phases :

- Une phase de préparation. Il s'agit notamment d'identifier les « porteurs d'usage » qui exprimeront le besoin, ou plus exactement le défi auquel répondront les participants, lesquels peuvent être des étudiants, des chercheurs, mais aussi des entreprises ;
- Une phase d'idéation. A partir des besoins exprimés, l'objectif est de permettre à des idées innovantes d'émerger autour de quelques projets montés par des équipes multidisciplinaires qui se structurent au fur et à mesure, souvent grâce à des plateformes online comme Agorize²³ ou BeMyApp²⁴ ;
- Une phase de prototypage. Les idées sont transformées en prototypes, voire en démonstrateurs. Le « livrable » demandé varie selon les hackathons mais il s'agit en général de présenter la réponse

²² <http://business.agorize.com/blog/transformation-digitale-top-et-flop-des-pratiques-internes-en-2017>

²³ <http://business.agorize.com/>

²⁴ <http://agency.bemyapp.com/organize-your-hackathon.html>

proposée non seulement sous la forme de « slides » mais aussi de quelques développements informatiques ;

- Une phase de présentation et d'évaluation. Cette phase débouche sur la désignation d'une ou plusieurs équipes vainqueurs qui se voient récompensées à la fois par une dotation financière et par l'accès à un programme d'incubation et d'accélération.

Le hackathon n'est en effet qu'un point de départ et en aucun cas un aboutissement : Il permet de détecter des idées innovantes qu'il s'agit ensuite de développer. Il est d'ailleurs essentiel d'établir un règlement précis déterminant les règles applicables en matière de propriété intellectuelle et de rétribuer, d'une façon ou d'une autre, non seulement le ou les gagnants, mais aussi les participants. Cette rétribution peut être financière ou « en nature », grâce à divers cadeaux et surtout au « mentoring » qui est apporté par le « porteur d'usage » et les différents experts (technologies, marché, droit...) qui encadreront les équipes. Cette rétribution est d'autant plus indispensable que certaines entreprises se voient aujourd'hui reprocher de récupérer à vil prix des idées innovantes, voire d'instrumentaliser les hackathons pour de simples raisons de communication. « L'authenticité » de la démarche est donc un critère clé du succès de l'opération... L'accompagnement du ou des gagnants par un programme d'incubation et d'accélération est par ailleurs fondamental si l'on souhaite éviter les « chasseurs de primes » et s'inscrire dans une perspective de long terme.

Incubation et accélération

De nombreux incubateurs et accélérateurs proposent désormais des programmes dédiés à l'accompagnement des start-ups. Première phase de 6 mois à 1 an, l'incubation permet de construire la solution grandeur réelle et de valider le modèle économique en plaçant l'entreprise dans un écosystème foisonnant et en fournissant des « mentors ». Ce n'est qu'ensuite que le projet pourra être « accéléré » avec l'aide de fonds d'amorçage pour se développer.

Cylon²⁵, incubateur européen dédié à la cybersécurité, a ainsi élaboré un programme d'incubation de 3 mois qui se traduit par un investissement de 15 000 livres dans chaque projet sélectionné en échange de 3 % du capital de chaque entreprise. Doté d'un conseil d'administration comprenant l'ancien patron du GCHQ, sir Iain Lobban, la structure est notamment sponsorisée par BAE Systems et Raytheon. Parmi les entreprises actuellement incubées : ThreatInformer, qui fournit aux souscripteurs des compagnies d'assurance des métriques leur permettant d'évaluer les risques, ou bien encore MyDocSafe, plateforme de e-signature. A noter que l'incubateur a opté pour une définition large de la cybersécurité lui permettant de travailler aussi bien dans les secteurs de la défense, de la distribution, des télécoms ou des *fin techs* dans des domaines variés (blockchain, conformité, assurance, protection des données personnelles, analytics, sécurité du cloud...).

Autre exemple de programme d'incubation et d'accélération : le GCHQ Cyber Accelerator²⁶. Géré par l'entreprise Wayra UK, filiale de Telefonica, ce programme est partie intégrante du Cyber Innovation Center mis en place à Cheltenham par le GCHQ et le *UK Department for culture, media and sport*. Les candidats doivent répondre à trois défis : sécurité des données (datamining, surveillance des réseaux et détection des

²⁵ <https://cylonlab.com/>

²⁶ <http://realbusiness.co.uk/tech-and-innovation/2017/01/11/cyber-security-startups-picked-government-led-accelerator/>

cyberattaques), sécurité des utilisateurs et sécurité des technologies²⁷. Les candidats retenus dans le cadre de ce programme bénéficient d'un accès aux expertises du GCHQ pour développer leurs capacités et améliorer leurs idées. Les start-ups y reçoivent une dotation financière mais aussi un accès à un espace de travail.

Cette phase d'incubation peut aussi s'appuyer sur des programmes d'expérimentation. La Région Bretagne, à travers la MEITO, a ainsi lancé en 2015 un programme qui a permis de financer à hauteur de 50 000 euros l'expérimentation de 11 solutions innovantes de cybersécurité²⁸. Présenté lors d'un petit déjeuner de l'Observatoire FIC en 2016, ce projet a pour objectif, en partant de l'expression de besoin d'un industriel, de créer un binôme offreur de solutions techniques – expérimentateur qui travaille pendant un temps relativement court (9-12 mois) au développement d'une solution répondant aux attentes de l'industriel. Objectif : permettre une mise sur le marché rapide d'une solution testée, l'expérimentateur jouant le rôle de premier « client ». A côté de l'incubation et de l'accélération de projets dans des lieux dédiés, ces programmes d'expérimentation apparaissent particulièrement pertinents, tant il est essentiel que les start-ups puissent très rapidement se confronter au marché. Des solutions de « résidence d'entreprise » permettant à des acteurs industriels d'héberger de façon temporaire, sur le modèle des résidences d'artiste, des « jeunes pousses » pourraient ainsi être imaginées.

Quelques exemples de hackathons centrés sur la « cybersécurité »

Plusieurs hackathons dédiés à la cybersécurité ont été organisés ces dernières années par des acteurs variés, entreprises, accélérateurs ou administrations.

- Startupbootcamp InsurTech : en juin 2016, l'incubateur londonien Startupbootcamp InsurTech dédié à l'assurance a organisé un hackathon²⁹ rassemblant des développeurs informatiques, des business developers et des designers organisés en équipes de 1 à 5 personnes. Le hackathon comprenait 4 défis (sécurité, protection des données personnelles, fraude, crime) portés chacun par une entreprise (PwC, MMI Holdings, Intesa Sanpaolo...) très opérationnels. Exemples : « détecter la fraude dans la cyber assurance » ou « cyber risk scoring ».
- Cyber Hack : en juin 2015, le Department of Business Innovation and Skills (BIS), administration britannique, en partenariat avec l'accélérateur londonien Accelerator Network, a organisé un hackathon de 3 jours réunissant 50 étudiants appartenant aux 13 centres d'excellence universitaires labellisés³⁰. Le gagnant a présenté une solution d'authentification multi-facteurs.
- General Electric : l'entreprise américaine a organisé en juin 2015 à Tel Aviv un hackathon dédié à la cybersécurité industrielle en partenariat avec l'Université de Tel Aviv³¹. Cet événement s'intégrait dans le cadre du renforcement des activités de l'entreprise dans la « start-up nation ».

²⁷ <https://wayra.co.uk/gchq/>

²⁸ http://www.meito.com/accueil/nos_services/financer_l_experimentation/appels_a_projets/73_469/experimentation_de_solutions_innovantes_de_cybersecurite

²⁹ <https://www.startupbootcamp.org/blog/2016/07/startupbootcamp-insurtechs-cybersecurity-hackathon-review/>

³⁰ <https://www.scmagazineuk.com/government-organises-cyber-security-hackathon/article/537421/>

³¹ <http://siliconwadi.fr/18260/general-electric-en-quete-de-cybersecurite-israelienne>

- Enel : l'énergéticien italien a organisé un premier hackathon sur la cybersécurité en octobre 2016³². Gagné par la société israélienne Aperio avec une solution de détection, le hackathon comptait 4 challenges : ICS, IoT, M2M, protection des données personnelles pour mobiles et app. Le nom du gagnant a été annoncé lors de l'édition européenne de l'événement israélien CyberTech. A noter que Enel dispose d'un hub innovation basé en Israël, dont l'objectif est de sélectionner chaque année une vingtaine de start-up qui seront ensuite accélérées.
- Cyber DiploHack : dans un genre très différent, les ministères hollandais de la justice et des affaires étrangères, et l'Ambassade des Pays-Bas en Grande-Bretagne, en partenariat avec le CSIS américain, ont organisé en mars 2015 un hackathon « politique » destiné à imaginer de nouvelles approches en matière de coopération internationale et de capacity building. Les résultats ont permis d'alimenter les réflexions de la Global Conference on Cyberspace organisée en avril 2015 à La Haye. A noter que l'un des prix a été remporté par la Chaire Castex de cyberstratégie³³.

Bonnes pratiques

Un hackathon dédié aux questions de cybersécurité pourrait s'articuler autour des éléments suivants :

- Définition de quelques verticales sectorielles (assurance, énergie, véhicule connecté, santé) ;
- Identification de « porteurs d'usage » susceptibles d'exprimer des besoins et d'accompagner dans la durée les projets ;
- Organisation de plusieurs événements dédiés à la présentation des défis, à l'idéation, au prototypage puis à la présentation des projets. Durée : d'une demi-journée à 2 jours sur une période de 4 mois, de façon à travailler en profondeur et à accompagner véritablement les équipes ;
- Utilisation d'une plateforme en ligne pour la constitution des équipes et pour les phases d'idéation et de prototypage ;
- Accompagnement des équipes par une équipe d'une dizaine de mentors (architectes, développeurs, juristes, business developers...) ;
- Sélection par le jury d'un projet par verticale. En récompense : dotation financière et accès à un programme d'incubation et d'expérimentation avec le « porteur d'usage » concerné.

³² <http://www.geektime.com/2016/12/13/aperio-systems-wins-enels-cyber-security-hackathon/>

³³ <http://www.diplohack.org/cyber-diplohack-washington-dc.html>

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.



Ministère de la Défense

Direction Générale des Relations Internationales et de la Stratégie

60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15



CEIS

Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15

Téléphone : 01 45 55 00 20

E-mail : omc@ceis-strat.com