
**Lettre n°66 - Septembre 2017 - disponible sur omc.ceis.eu**

Brève du mois

**« Nous avons besoin d'une agence plus puissante. Nous sommes de plus en plus confrontés à un défi représenté par les attaques hybrides mêlant les cybermenaces à d'autres techniques »**[1] - Julian King, commissaire européen à la Sécurité, au sujet du projet de renforcement de l'ENISA de la Commission Juncker.

## TABLE DES MATIERES



[1] https://www.lecho.be/economie-politique/europe-general/L-Europe-se-dote-d-une-Agence-de-cybersecurite/9933976

# GEOPOLITIQUE DES PUISSANCES DE CALCUL

Le 23 mars 2017, les ministres de sept pays européens ont signé un accord pour le démarrage d'un programme appelé EuroHPC qui devra aboutir à des supercalculateurs exaflopiques, c'est à dire capables de traiter au moins $10^{18}$ calculs par seconde. Ce programme, qui devra englober les initiatives européennes actuelles et futures participant à cet objectif, fait écho aux nombreuses initiatives similaires à travers le monde dans la course à l'exaflop.

## Les besoins en informatique de haute performance

### Simulation :

La puissance de calcul constitue le plus grand frein à la simulation de systèmes complexes. Chaque facteur à prendre augmentant exponentiellement la complexité des calculs, la quête de supercalculateur toujours plus puissant est associée au développement technologique. Elle concerne notamment :

- La météorologie (et évolutions climatiques) ;
- L'armement. L'utilisation de supercalculateurs pour le développement d'armement nucléaire constitue l'une des premières justifications des restrictions à l'exportation des technologies et matériels associés ;
- L'énergie : nucléaire, énergies renouvelables (terrains complexes, météorologie), etc. ;
- Ingénierie analytique : Recherche de nouveaux matériaux ; Développement de véhicules (terrestres, maritimes, aériens, spatiaux…). Les constructeurs ont de plus en plus recours à la simulation, qui permet de fortement diminuer le besoin de production de prototypes[2]. L'augmentation des capacités de calcul encourage ce recours, permettant des simulations plus réalistes (car pouvant prendre en compte davantage de facteurs) ;
- La médecine de précision (recherche de traitement, médecine personnalisée et prédictive).

### Intelligence artificielle

La puissance de calcul constitue l'un des trois leviers de l'intelligence artificielle, avec les données et les techniques d'apprentissage et de traitement de vastes échantillons de données (*Machine Learning*, *Data Mining*, *Big Data*, moteurs d'inférence déductifs, etc.). Pour ces systèmes, une plus grande puissance de calcul permet de prendre en compte davantage de facteurs ou de tester davantage de scénarios, ce qui permet d'obtenir une décision plus fiable.

Certaines applications de l'IA, telles que l'aide à la décision dans le domaine médical, nécessitent pour leur fonctionnement une puissance de calcul relevant ou s'apparentant à des systèmes de type supercalculateur. D'autres applications, comme la conduite autonome, peuvent fonctionner avec des ressources plus faibles (conséquence de la contrainte de matériel embarqué). Cependant, même pour ces systèmes, la phase d'apprentissage (l'entraînement des réseaux de neurones) impliquera toujours l'utilisation de systèmes HPC.

[2] Le recours au HPC a permis aux constructeurs européens de réduire le temps de développement de nouveaux véhicules terrestres de 60 à 24 mois. Il permet de rendre les véhicules plus performants : efficacité énergétique, réduction du bruit, etc.

## Cybersécurité / Cyberdéfense

Une application phare des calculateurs militaires est la cryptanalyse, et plus spécifiquement le calcul de clé privée à partir de clé publique. Si le choix de la taille des clés de chiffrement vise à rendre prohibitif ce travail de cryptanalyse, la connaissance de failles dans les protocoles ou dans leur implémentation peut rendre ces techniques viables. Ce type de calcul étant hautement parallélisable, il n'est pas nécessaire d'avoir recours à des supercalculateurs d'architecture monolithiques (non distribuée) : on peut au contraire tirer parti d'une architecture parallélisant un grand nombre de systèmes standards. La cryptanalyse a ainsi beaucoup recours au GPU Computing[3].

Dans le domaine de la recherche, il est également possible d'employer des systèmes HPC pour étudier et simuler de façon dynamique des menaces informatique. Cela a par exemple été expérimenté pour la simulation de botnets, grâce à la mobilisation d'un grand nombre de machines virtuelles, afin de mieux les comprendre et les repérer[4].

S'agissant de la protection opérationnelle contre les menaces, l'intégration au sein des solutions de sécurité d'intelligence artificielle, notamment sous la forme d'UEBA[5], c'est-à-dire d'analyse du comportement des entités (malwares) et des utilisateurs (y compris pour l'authentification), offre une solution à la multiplication et à la sophistication des menaces. Aujourd'hui, nombre d'entreprises indiquent intégrer des capacités d'apprentissage automatique (*Machine Learning*), mais il est difficile d'évaluer le niveau de sophistication des algorithmes en question. L'apprentissage automatique impliquant l'allocation de capacités de traitement en adéquation avec la complexité de l'environnement et de ses entités, on peut cependant prédire une augmentation du besoin en informatique haute performance pour les solutions de sécurité type SIEM/IDS, c'est à dire pour :

- L'analyse de malware, qui implique d'instancier des environnements virtuels en temps réel afin de tester chaque fichier/processus suspecté. Cela permet en outre de collecter des traces d'exécution qui seront autant d'éléments de comparaison pour des analyses ultérieures ;
- Le monitoring réseau / la détection de menaces.

En comparaison des autres domaines, le secteur de la cybersécurité reste aujourd'hui peu mature s'agissant de l'utilisation des ressources HPC au service de la détection des menaces et de la protection des réseaux.

## Typologies HPC

Le *High Performance Computing* (HPC) vise à agréger des capacités de calcul pour obtenir un système global capable de traiter des calculs qu'un ordinateur classique ne serait pas en mesure de traiter.

On peut distinguer deux catégories de HPC :

---

[3] Le GPU Computing correspond à l'utilisation de la puissance de calcul des cartes graphiques (matériel originellement destiné à générer des rendus 3D) pour des tâches hautement parallélisables (un très grand nombre de calculs relativement petits).

[4] https://www.osti.gov/scitech/biblio/1141631-emulytics-large-scale-emulation-botnets

[5] UEBA : User and Entity Behavior Analytics

- D'un côté, le Commodity Computing : il s'agit d'utiliser un grand nombre de composants standards (Commodity Hardware) afin d'obtenir le meilleur ratio performance/coût. L'environnement logiciel employé est le plus souvent également standard. C'est la voie choisie pour l'Utility Computing[6] (et donc, de façon générale, les solutions dans le Cloud). Les systèmes relevant du Commodity Computing sont généralement conçus avec l'idée qu'une multitude d'utilisateurs soumettent des problèmes qui ne nécessitent qu'une fraction de la puissance totale du cluster ou du grid[7].
- De l'autre, un HPC qui prend la forme de supercalculateurs monolithiques destinés à des utilisations très spécifiques, qui favorisent la performance de pointe au détriment de la facilité de programmation (et donc de souplesse d'utilisation). Contrairement au Commodity Computing, ces systèmes sont peu évolutifs.

La question du choix de l'architecture n'est pas uniquement dictée par le coût. Il faut savoir si le problème à traiter peut être découpé en une multitude de problèmes indépendants. Dans le cas contraire, ils nécessiteront une capacité de mémoire unifiée maximale ainsi qu'une très grande bande passante inter unité de calcul, ce qui correspondra aux architectures de type supercalculateur. Pour ces raisons, l'emploi de supercalculateur est nécessaire pour les simulations de systèmes complexes

Pour la recherche, l'une des principales utilisations du HPC, la question de la disponibilité est également primordiale. L'expert en HPC Geoffrey Fox de l'Université d'Indiana expliquait que pour un chercheur, la différence de disponibilité des ressources en Cloud permettait souvent aux chercheurs d'obtenir leurs résultats plus rapidement qu'avec des supercalculateurs, dont les listes d'attente peuvent être particulièrement longues. Cette question d'accès à la puissance de calcul a fait émerger la notion de Jungle Computing, qui consiste à mettre à profit la puissance de calcul de sources très hétérogènes : serveurs, ordinateurs personnels (processeur et carte graphique), consoles de jeux… Un certain nombre de projets de recherche se sont bâtis selon ce type d'architecture, certains sous forme d'informatique volontaire : les participants installent un programme permettant de mettre à disposition des chercheurs les ressources non utilisées de leur ordinateur. Si un utilisateur utilise 15% de la puissance de calcul de son ordinateur pour ses activités, les 85% restants peuvent ainsi être mis à profit de la recherche médicale (Rosetta@home, FightAIDS@Home), fondamentale (LHC@Home), spatiale (SETI@Home), etc.

[6] L'*Utility Computing* est un modèle de service visant à mettre à disposition des clients des ressources computationnelles en fonction de leur besoin, avec une facturation correspondant à l'usage effectif. Les entreprises leaders dans ce domaine offrent aujourd'hui aux entreprises et organisations des capacités HPC dans le Cloud pour les utilisations citées en première partie.

[7] Un *Cluster* (grappe) est un regroupement d'un certain nombre d'ordinateurs proches travaillant de concert de façon à ne former qu'un seul système. Les nœuds d'une grappe traitent une seule et même tâche en parallèle.
Le Grid (grille) est un regroupement d'un certain nombre d'ordinateurs, le plus souvent éloignés géographiquement, en vue de traiter un problème commun. Les nœuds d'une grille sont généralement utilisés pour traiter des tâches distinctes.

## États-Unis

Le 29 juillet 2015, le président Obama signait une ordonnance pour la création du NSCI (National Strategic Computing Initiative), une initiative aujourd'hui implémentée par l'Exascale Computing Project qui vise à :

- Accélérer le développement des technologies nécessaires pour atteindre des puissances de calcul exaflopiques (un milliard de milliard d'opérations par seconde) ;
- Développer l'écosystème HPC national ;
- Développer les collaborations public-privé afin de partager les bénéfices des avancées R&D à l'ensemble des parties prenantes (gouvernement, industrie et secteur académique) ;
- Accroître la cohérence entre les technologies employées pour la modélisation et la simulation et celles employées par l'analyse de données.

Le 15 juin 2017, le ministère américain de l'énergie a décidé de financer à hauteur de 258 millions de dollars un ensemble de programmes de recherches d'entreprises technologiques, toujours dans le cadre du programme « Pathforward » de l'Exascale Computing Project. HP, IBM, Intel, Nvidia, AMD et Cray devront financer eux-mêmes 40% du coût total de leur projet, amenant l'investissement total à un minimum de 430 millions de dollars.

La position historiquement dominante des États-Unis dans le domaine du HPC est l'un des atouts décisifs du pays dans la compétition technologique mondiale. L'initiative du 29 juillet 2015 mentionnait que les États-Unis reconnaissaient d'ailleurs que ses hauts niveaux d'investissements dans ce domaine avaient contribué significativement à la recherche scientifique et, par conséquent, à la prospérité économique du pays. La suprématie dans les composants matériels lui permet également de conditionner le développement de l'écosystème HPC des autres pays, du moins pendant un temps. Les États-Unis limitent par exemple l'exportation des puces les plus performantes lorsqu'ils soupçonnent leur utilisation à des fins militaires, notamment pour le développement d'armements nucléaires.

Le 8 mars 2013, le BIS (Bureau of Industry and Securities, US Department of Commerce) ajoute ainsi l'entreprise russe T-Platforms à sa liste d'organisations qui « agissent de façon contraire à la sécurité nationale ou aux intérêts extérieurs des Etats-Unis ». Une telle décision implique en effet que toute exportation à destination des entités présentes sur la liste soit soumise à une autorisation, rarement accordée, du BIS. Pour T-Platforms, fabriquant russe de supercalculateur, l'impact de cette décision a été lourd[8] car l'entreprise importait nombre des composants de ses supercalculateurs, notamment les microprocesseurs, à des sociétés américaines.

De même, en avril 2015, l'US Department of Commerce a refusé l'exportation de processeurs haute performance d'Intel pour le Tianhe-2 et trois autres supercalculateurs chinois, au motif que ceux-ci avaient été utilisés pour des activités liées au nucléaire militaire[9]. L'instance américaine est même allée plus loin en interdisant la vente de GPU haut de gamme à destination des centres de recherche chinois. La pertinence

[8] http://primeurmagazine.com/weekly/AE-PR-02-14-32.html

[9] https://www.bis.doc.gov/index.php/forms-documents/regulations-docs/federal-register-notices/federal-register-2015/1196-80-fr-8524/file

des limitations à l'export de ce type de matériel fait cependant débat. Si les États-Unis ont toujours souhaité garder l'avantage, les restrictions à l'exportation se sont réduites au cours des années 90, au plus grand bénéfice de l'industrie du pays. Avec l'augmentation continue de la puissance de calcul intégrée aux processeurs, les stratégies de limitation et de sanction ne peuvent en effet permettre, au mieux, que de garder une courte avance, lorsqu'elles ne sont pas tout simplement contournées à travers des sociétés écrans. Quid, enfin, du contrôle quasi impossible de l'utilisation des ressources HPC dans le *Cloud* ?

Principales entreprises / organisations publiques HPC américaines : IBM, Cray, Raytheon BBN Technologies, Northrop Grumman, HPE, NGI, Dell.

**Chine**

Á travers son treizième plan quinquennal, la Chine vise l'exaflopique d'ici la fin 2020 dans le cadre de son programme 863, programme initialement lancé en 1986 avec pour objectif de stimuler le développement de technologies avancées visant à rendre la Chine indépendante des technologies étrangères. Pour atteindre cet objectif, le pays investit dans la recherche et le développement en matière de puce 3D, d'interface d'interconnexion et de photonique sur silicium[10].

La Chine a depuis quelques années accéléré les investissements en matière d'HPC, à tel point que le taux d'utilisation des supercalculateurs chinois est généralement inférieur à celle des autres pays, la demande en supercalculateur y étant inférieure à l'offre. La Chine se dispute aujourd'hui le leadership dans le domaine des supercalculateurs avec les États-Unis en termes de nombre de supercalculateurs dans le TOP500 et de puissance de calcul agrégée[11]. Alors qu'elle ne classait aucun système dans le Top 500 en 2001, la Chine en compte aujourd'hui 160 (contre 168 pour les États-Unis) et possède les deux supercalculateurs les plus puissants du monde.

Même si la majeure partie des supercalculateurs chinois utilisent du matériel américain (Intel, Nvidia…), son plus puissant supercalculateur (qui est incidemment le plus puissant au niveau mondial) utilise des puces purement chinoises de type Sunway. Elles sont développées par le *Jiangna Computing Lab*, qui développe ces puces depuis 2006 pour la PLA (*People Liberation Army*).

Principales entreprises / organisations publiques HPC chinoises : Lenovo, Inspur, Huawei, Sugon (aussi connue sous le nom de Dawning), NRCPC, NUDT.

**Japon**

Le Japon a montré son intérêt pour le domaine HPC, ayant par deux fois déjà possédé le supercalculateur le plus puissant. Il semble cependant incapable de maintenir un niveau d'investissement constant permettant de rivaliser avec les États-Unis ou la Chine. Le Japon a favorisé le développement de processeurs locaux pour ses flagships, à l'instar du K-Computer qui embarque des processeurs dédiés Fujitsu. Celui-ci était à la première place du classement Top500 à sa mise en service en juin 2011 et reste à la huitième place 6 ans plus tard, démontrant si besoin était la capacité du Japon de s'affranchir des puces américaines.

[10] https://www.hpcwire.com/2016/05/02/china-focuses-exascale-goals/

[11] https://techcommunity.ts.fujitsu.com/en/servers-2/d/uid-37c539ec-d137-c4c6-d9b5-2dab9a8ccf99.html

Le Japon prévoit l'arrivée de son premier supercalculateur de niveau exaflopique pour 2020, un système qui sera destiné à Riken, le prestigieux institut de recherche nippon. Le supercalculateur en construction, baptisé Post-K[12], est développé par Fujistu mais exploitera des processeurs ARM.

Principales entreprises / organisations publiques HPC japonaises : Jujitsu, NEC, Hitachi.

**Russie**

Même si le pays a cherché à stimuler sa propre industrie de semi-conducteur pour faire face aux restrictions à l'exportation des puces américaines, ses investissements dans le domaine HPC se sont effondrés ces dernières années malgré des besoins toujours aussi grands[13]. Une probable conséquence des sanctions économiques qui poussent le pays à faire des compromis. Jusqu'en 2012, le pays prévoyait d'investir 1,5 milliard de dollars dans le développement de supercalculateurs exaflopique, dont 250 millions pour la création d'un centre qui doit développer les ASICs russes à cet effet. L'idée, émise en 2014, d'un partenariat avec l'Inde pour le co-développement de technologies HPC n'a pour l'heure pas non plus pris forme.

La Russie possèderait cependant le plus puissant supercalculateur dédié à une utilisation militaire, en tout cas parmi les pays qui en font état. Le supercalculateur du NDMC (National Defense Management Center[14]) possèderait ainsi une puissance de 16 Petaflops[15] et serait, selon les dires du Ministre de la Défense russe Sergey Choïgou, utilisé à des fins de simulation et d'anticipation des conflits actuels et futurs[16].

Principales entreprises / organisations publiques HPC russes : T-Platforms, RCS Group, Niagara.

**Inde**

L'Inde a consenti à allouer 2 milliards de dollars à l'Indian Space Research Organisation et à l'Indien Institute of Science pour développer un supercalculateur « high-end » d'ici 2018. L'agence gouvernementale C-DAC (Centre of Development of Advanced Computing) a également annoncé un programme de 670 millions de dollars pour le développement de 70 supercalculateurs[17].

L'Inde a commencé à développer son premier supercalculateur après s'être vue imposer un embargo sur les armes par les États-Unis, qui comprenait le domaine du HPC en tant que technologie duale pouvant être employée à développer des armes nucléaires. Son premier superordinateur, démarré en 1991, avait été dupliqué en Russie dans le cadre d'une collaboration entre les deux pays. En 2007, l'Inde a produit un

[12] http://www.fujitsu.com/global/Images/post-k-supercomputer-overview.pdf
http://www.aics.riken.jp/en/k-computer/about/

[13] https://www.nextplatform.com/2016/01/05/a-strange-state-for-the-russian-supercomputing-industry/

[14] Le National Defense Management Center est le plus haut centre de Command & Control du Ministère de la Défense russe.

[15] Ce qui placerait ce supercalculateur à la sixième place dans le classement Top500

[16] http://www.cyberlightglobal.com/russian-military-preps-cyber-warriors/
https://www.rt.com/news/372375-russian-military-supercomputer-pentagon/

[17] https://www.hpcwire.com/2014/04/09/russia-india-explore-joint-supercomputing-project/

supercalculateur, Eka (qui signifie numéro un en Sanskrit), qui était à la quatrième place mondiale et à la première place en Asie au moment de sa sortie.

Principales entreprises / organisations publiques HPC indiennes : C-DAC, Netweb, Wipro.

**Union Européenne**

L'Union Européenne possède quelques constructeurs de supercalculateurs, dont le plus important est indéniablement Bull, mais son industrie n'est pas à l'échelle de ses besoins. Alors que celles-ci contribuent à hauteur de 5% des ressources HPC au niveau mondial, l'Union Européenne consomme un tiers des ressources mondiales[18].

Le 23 mars 2017, les ministres de sept pays européens (Allemagne, France, Italie, Luxembourg, Pays-Bas, Portugal et Espagne) ont signé un accord pour le démarrage d'un programme appelé EuroHPC qui devra aboutir à des supercalculateurs exaflopiques.

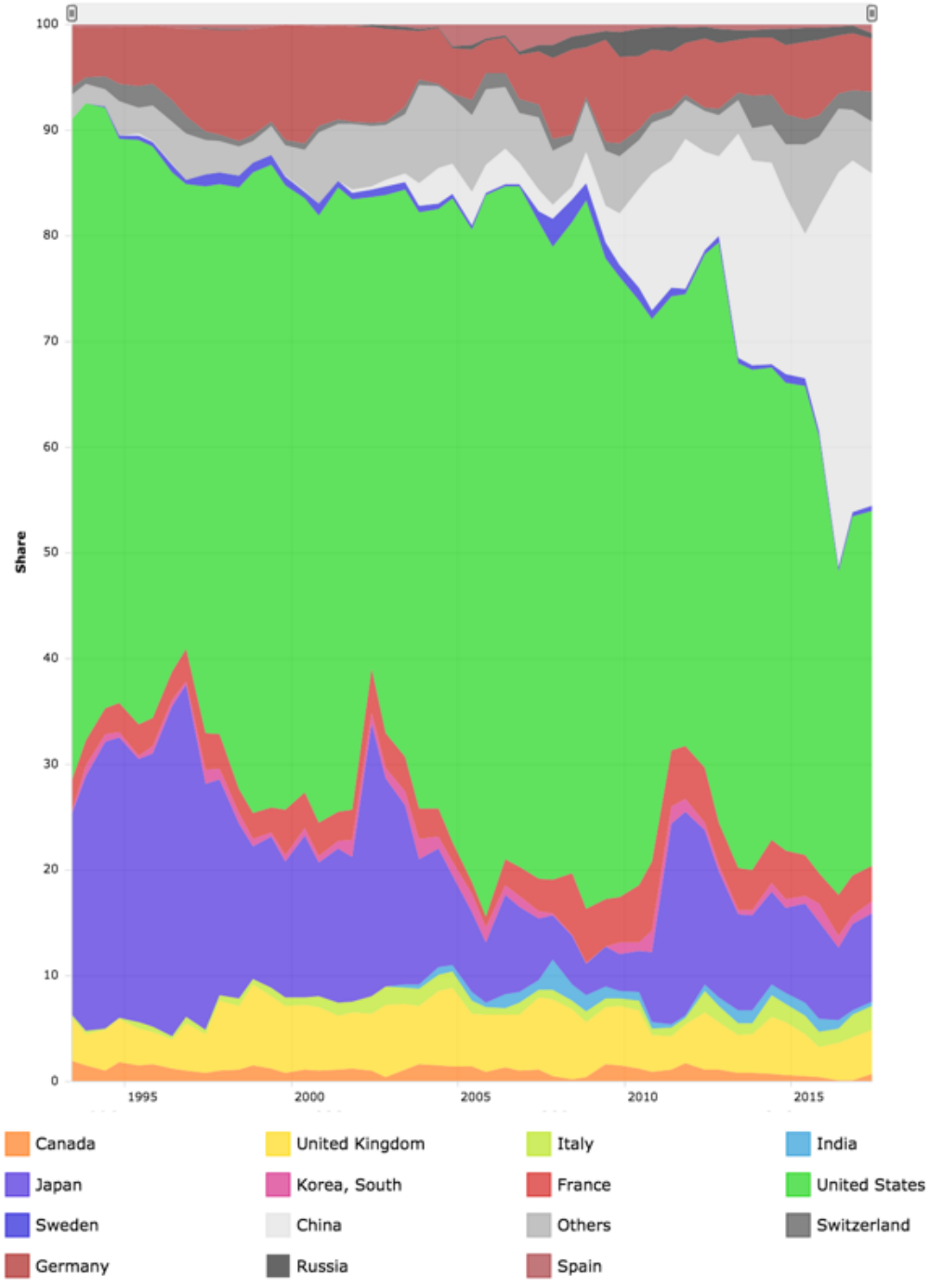
La Belgique et la Slovénie ont depuis rejoint le projet[19].

Principales entreprises / organisations publiques HPC européennes : Bull, Eurotech, Clustervision, Xenon.

[18] https://ec.europa.eu/digital-single-market/en/news/eu-ministers-commit-digitising-europe-high-performance-computing-power

[19] http://eurohpc.eu/

**Evolution de la part de la puissance de calcul des différents pays au sein du TOP500**
(Source : TOP500)




Note : la représentativité du Top500 en matière de puissance de calcul possède plusieurs limites. En premier lieu, seuls sont considérés les systèmes volontairement inscrits, ce qui exclut par exemple les systèmes militaires. Les systèmes relevant de l'*Utility Computing* n'y sont pas intégrés non plus.

## Conclusion

Le développement de technologies exaflopiques n'a pas simplement pour objectif de posséder les supercalculateurs les plus puissants du monde. D'une part, il s'agit d'être autonome dans la maîtrise de ces technologies afin de s'assurer un accès pérenne à ces ressources. D'autre part, le processus de développement de technologies exaflopiques permet de générer une propriété intellectuelle susceptible de nourrir d'autres produits informatiques : smartphones, systèmes embarqués, serveurs, etc. En effet, les avancées technologiques dans le domaine du HPC (*High Performance Computing*) se retrouvent régulièrement dans le marché grand public quelques années après leur introduction dans les supercalculateurs.

La maîtrise des technologies HPC est donc devenue une priorité stratégique pour les nations les plus puissantes. Celles qui ne développent pas de programme similaire courent le risque de se voir distancer technologiquement dans de nombreux domaines.

## Références


- Sur les programmes régionaux de développement du HPC (jusqu'en 2016) : https://ec.europa.eu/digital-single-market/en/news/staff-working-document-implementation-action-plan-european-high-performance-computing-strategy

# PROGRAMMES BUG BOUNTY : UNE SOLUTION POUR SECURISER LES PLATES-FORMES A MOINDRE COUT

Au cours des dernières années, de nombreuses entreprises du numérique ont franchi le pas du *Bug Bounty.* Objectif : mettre au défi pirates informatiques (*Whitehats*[20]*)* et chercheurs en sécurité de détecter au sein de leurs produits des bugs, notamment ceux constituant des vulnérabilités, reconnaissance et récompense pécuniaire à la clé[21]. Une condition : les rapports de vulnérabilités doivent être suffisamment documentés pour que l'organisation puisse reproduire l'exploitation de la vulnérabilité et la corriger par la suite.

Cette approche, qui peut sembler contre-intuitive (inciter le « piratage » pour mieux s'en protéger) ne cesse de prendre de l'ampleur outre-Atlantique. GAFAMs, spécialistes réseau (Netgear, Cisco…), éditeurs d'antivirus, e-commerce, etc. intègrent désormais cette démarche dans le cycle de vie de leurs produits. Le *Bug Bounty* tend en effet à devenir la règle parmi les grandes entreprises du numérique[22] et les récompenses sont régulièrement revues à la hausse. Récemment, Google a augmenté sa récompense sur ses domaines Google, Youtube et Blogger de 20.000$ à plus de 30.000$ (plus un bonus de 1.337$[23]). Microsoft a également doublé ses primes de 15.000$ à 30.000$[24].

## Principe de fonctionnement

Les programmes de *bug bounty* peuvent être publiés sur le site web de l'entreprise concernée ainsi que sur des plates-formes dédiées. Ces plates-formes regroupent toutes les entreprises qui ont décidé de mettre leurs sites web ou applications sur un programme commun et font la liaison entre les chercheurs de sécurité et les entreprises. Parmi les plates-formes les plus connus, on peut notamment citer HackerOne[25], Bugcrowd[26] et BountyFactory[27] pour l'Europe. HackerOne est l'une des premières entreprises à avoir fait de la *crowd-sourced*[28] *security* la base de son modèle économique. Avec 100 000 hackers, plus de 20 millions de dollars

[20] Un *Whitehat* est un *hacker* éthique ou un expert en sécurité informatique qui réalise des tests d'intrusion et des actions de *reverse engineering* afin d'assurer la sécurité d'un équipement ou d'un système d'information. Ils s'opposent aux *blackhats*, qui sont les *hackers* mal intentionnés.

[21] En règle générale, les montants des paiements correspondent à la taille de l'organisation, à la difficulté à pirater le système et à l'impact sur les utilisateurs d'un bug.

[22] https://www.bugcrowd.com/bug-bounty-list/

[23] En référence au terme « *leet* » (dont l'écriture alternative est *1337*), dérivé du mot élite. Celui-ci est utilisé comme adjectif pour décrire une prouesse dans le domaine du hacking.

[24] https://blogs.technet.microsoft.com/msrc/2017/07/26/announcing-the-windows-bounty-program/

[25] https://www.hackerone.com/

[26] https://www.bugcrowd.com/

[27] https://bountyfactory.io/fr/index.html

[28] Crowdsourcing, littéralement « employer la foule » consiste à se tourner vers un groupe de personnes pour obtenir les connaissances, les biens ou les services nécessaires.

de primes redistribués pour 883 programmes de *Bug Bounty* et plus 53.000 bugs corrigés, elle était en septembre 2017 la première entreprise du genre.

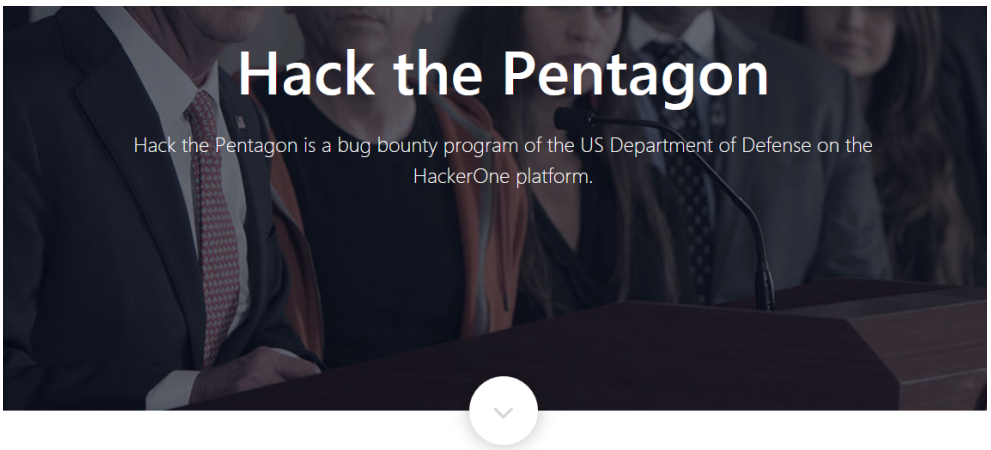
**Comment ça marche ?**

Les entreprises publient sur une plate-forme de *Bug Bounty,* ou bien sur leur propre site, leur politique concernant le programme. Cette politique définit le périmètre et les vulnérabilités acceptées par l'entreprise. Quand le chercheur trouve une vulnérabilité, il soumet un rapport sur la plate-forme de *Bug Bounty* ou bien sur le site web de l'entreprise. Le rapport doit inclure une description détaillée de la vulnérabilité découverte avec des étapes concrètes et concises ou une « preuve de concept ». Si le chercheur n'explique pas la vulnérabilité en détail, l'entreprise peut refuser de le récompenser.

## Principaux programmes

**Etats-Unis**

En mars 2016, le gouvernement américain a lancé le programme « *Hack the Pentagon* »[29] en utilisant la plate-forme HackerOne. Le programme de 24 jours a permis la découverte et la correction de 138 vulnérabilités dans les sites Web du ministère de la Défense (*DoD*), avec plus de 70 000 $ de primes versées aux pirates informatiques.

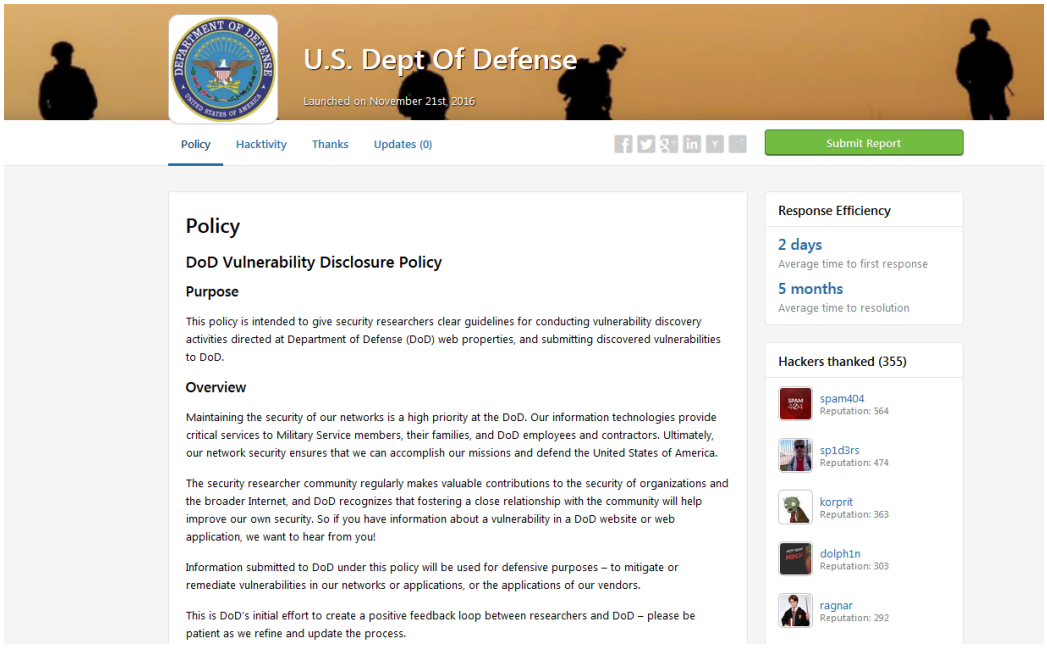



Hack the Pentagon is a bold security initiative by the US Department of Defense on the HackerOne platform. Over the next three years HackerOne and DoD will partner to bring crowdsourced security initiatives to other departments.

En octobre de la même année, le DoD a défini une politique de divulgation de vulnérabilité (VDP), la première de son genre créée pour le gouvernement américain. Cette politique a été mise en application pour la fois dans le cadre de l'initiative *« Hack the Army »*[30].

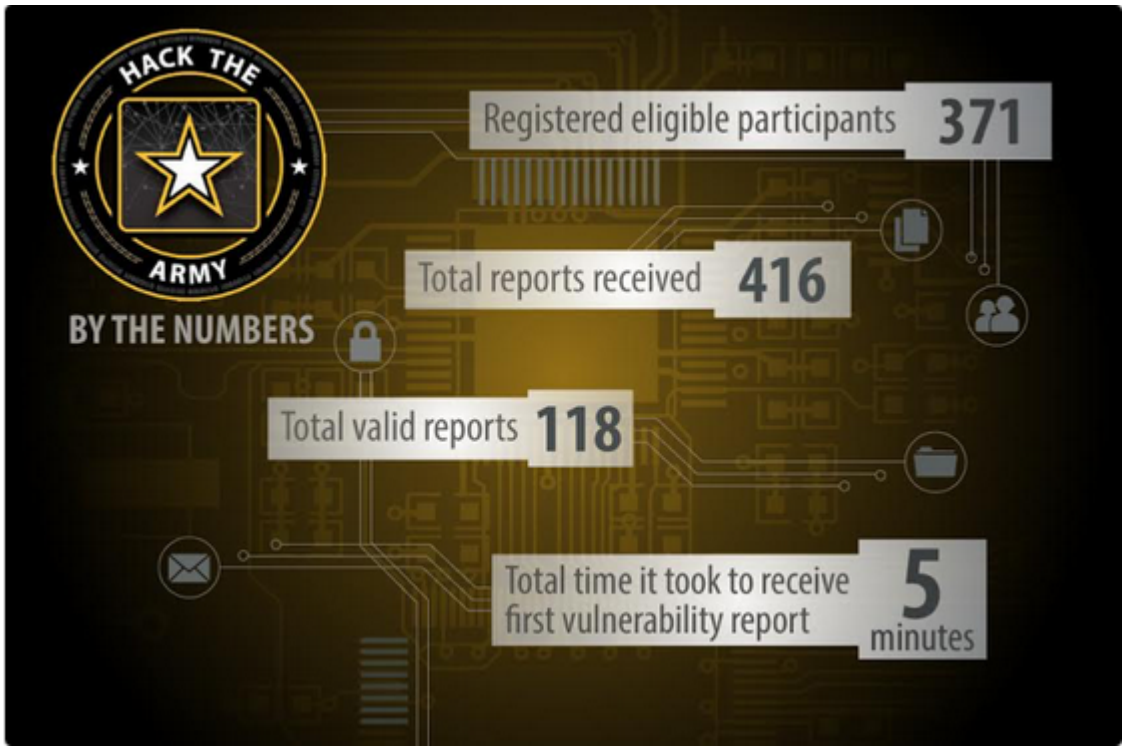
[29] https://www.hackerone.com/resources/hack-the-pentagon

[30] https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In




Le programme *« Hack the Army »* a produit 118 rapports de vulnérabilité valides et a vu participer 371 personnes, dont 25 employés du gouvernement et 17 militaires. Les *hackers* ont récolté au total environ 100 000 $ en récompense.

Selon HackerOne, le point le plus critique était due à l'exploitation combinée de plusieurs vulnérabilités, qui a permis aux *hackers* de se rendre sur un site interne du DoD depuis un site Web public (goarmy.com).




Suite au succès des opérations *« Hack The Pentagon »* et *« Hack The Army »,* le DoD a lancé le programme *« Hack The Air Force »*[31] en juin 2017.

« Les adversaires tentent constamment d'attaquer nos sites Web. Les secondes opinions sont les bienvenues - et dans ce cas, des centaines de secondes opinions - sur la santé et la sécurité de notre infrastructure en ligne pour anticiper et nous donner plus de détails sur la manière de protéger nos systèmes », explique Peter Kim, responsable de la sécurité des systèmes d'information de l'US Air Force

Même si l'opération a suscité quelques réticences en interne, son rapport coût/efficacité a semble-t-il convaincu. « L'avantage de s'ouvrir à des programmes comme celui-ci est de pouvoir obtenir d'excellents résultats pour de faibles coûts », soulignait Chrys Lynch, directeur du service de défense du numérique à l'US Air Force.

Le périmètre du *bug bounty* est cependant limité puisque celui-ci ne porte que sur des applications web comme les sites de recrutement et non sur des systèmes d'armement ou plates-formes critiques pour la sécurité nationale. Par ailleurs, seuls des experts en sécurité de nationalité américaine, ou ceux du Royaume-Uni, de Nouvelle-Zélande, d'Australie et du Canada peuvent participer au programme.

Au total, cette campagne a permis, selon les statistiques officielles publiées par l'US Air Force et HackerOne, de révéler 207 failles de sécurité du 30 mai au 23 juin 2017 pour plus de 130.000$ de récompenses (*bounties)*.

[31] https://hackerone.com/hacktheairforce

**Russie**

Même s'il ne s'agit pas à proprement parler d'un bug bounty, le gouvernement russe a lancé en 2014 un programme offrant près de 4 millions de roubles (environs 111 000 $) à qui pourrait concevoir et développer une technologie fiable pour déchiffrer les données envoyées sur le réseau Tor (un réseau d'anonymat chiffré notamment utilisé par les internautes afin de cacher des activités illégales).

Le ministère russe des Affaires intérieures (MIA) a ainsi indiqué sur son site officiel[32] qu'il souhaitait que les chercheurs étudient la possibilité d'obtenir des informations techniques sur les utilisateurs et leurs équipements. Seuls les ressortissants et les entreprises russes étaient autorisés à participer à la compétition "afin d'assurer la défense et la sécurité du pays". Les participants devaient en outre payer des frais d'inscription de 195 000 roubles (environ 5 555 $) pour participer au concours.

**Europe**

Les premières plates-formes de Bug Bounty, telles que BountyFactory[33] ou Yogosha[34], sont arrivées en Europe quatre ans après les premières plates-formes américaines, et les entreprises du vieux continent en sont aux expérimentations.

BountyFactory fait partie du projet *Yes We Hack*, qui propose trois plates-formes interconnectées : une plate-forme d'emploi dédiée à la sécurité des SI, qui se considère la première de son genre ; une plateforme de *Bug Bounty*, qui recense les programmes *Bug Bounty* publics et enfin un générateur de programme de *Bug Bounty* qui est la première plate-forme de *Bug Bounty* européenne, « BountyFactory »[35].

## Un programme Bug Bounty qui a dérapé

En 2013, un chercheur en sécurité informatique originaire de Palestine a trouvé un bug sur Facebook permettant à quiconque de poster sur le mur d'un autre utilisateur. Le chercheur a essayé de notifier le problème à l'équipe de sécurité de Facebook à plusieurs reprises mais n'a pas eu de réponse. Il a alors décidé de publier le bug sur le mur de Mark Zuckerberg. Facebook a répondu qu'il ne s'agissait pas d'un bug et a refusé de remettre une récompense en raison de la divulgation publique de la faille. La communauté des hackers éthiques a alors pris les choses en main et a recueilli plus de 13.000$[36] pour compenser le chercheur pour ses efforts.

[32] http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008

[33] https://bountyfactory.io/fr/index.html

[34] https://www.yogosha.com/

[35] https://yeswehack.com/fr/yeswehack.html

[36] https://www.gofundme.com/3znhjs

## Conclusion

Les programmes de *Bug Bounty* offrent la possibilité aux entreprises d'externaliser la recherche de vulnérabilités en collectant un nombre significatif de failles de sécurité potentielles qui seront reproduites et analysées, et ce afin de permettre l'amélioration du code. Avec un bon programme de *Bug Bounty*, une entreprise peut faire tester la sécurité de son site ou de ses applications en continu par des centaines d'experts avec une diversité de compétences dans la sécurité des systèmes informatique et à faible coût. Bien que l'utilisation de *hackers* éthiques pour trouver des vulnérabilités puisse être très efficace, ces programmes peuvent cependant susciter des inquiétudes car la vérification de l'honnêteté de ces hackers est impossible et ils peuvent utiliser les vulnérabilités découvertes à des fins malicieuses. Pour limiter les risques potentiels, certaines organisations proposent des programmes fermés de B*ug Bounty* nécessitant une invitation. Apple, par exemple, a limité la participation à ses programmes à quelques dizaines de chercheurs.

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 des Armées**
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.eu