IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

www.irsem.fr

Brève stratégique - 89

3 avril 2026

Fragmentation ou complémentarité ?

Le rôle de l'Union européenne (UE) dans la gouvernance des vulnérabilités informatiques

Jeanne-Louise Roellinger

Le Global CVE Allocation System, soutenu par l'UE, a été lancé début janvier. Cet événement fait suite aux problématiques de financement du programme CVE, opéré par MITRE Corporation et soutenu par le gouvernement américain. L'initiative illustre la manière dont l'UE affirme son influence normative tout en atténuant sa dépendance aux infrastructures non européennes. Cette dimension prend toute son importance à l'heure du retour de la compétition entre grandes puissances.

Le 7 janvier dernier, le Global CVE Allocation System (GCVE) a annoncé publiquement le lancement d'une nouvelle base de données publique recensant les vulnérabilités informatiques. Soutenue financièrement par l'UE, la publication intervient après un épisode d'incertitude relative à la continuité du programme CVE (*Common Vulnerabilities and Exposures*), le référentiel en matière d'identification standardisée des vulnérabilités. Le programme est opéré depuis 1999 par MITRE, une organisation à but non lucratif soutenue par le gouvernement américain, et constitue **l'autorité en termes de référencement des vulnérabilités** auprès des distributeurs de logiciels, des agences de cybersécurité, ainsi que des communautés de recherche en sécurité informatique. La survie du programme CVE et le GCVE soulèvent aussi bien des questions de résilience, d'interopérabilité, que de confiance et de souveraineté. Les tensions croissantes au sein des relations transatlantiques conduisent à s'interroger, d'une part, sur leurs implications pour l'autonomie européenne et, d'autre part, sur la possibilité qu'elles signalent une fragmentation de la gouvernance des vulnérabilités.

Les discours sur la fragmentation tendent à émerger précisément quand les problématiques de souveraineté font surface. Dans le domaine de la cybersécurité spécifiquement, les appels à préserver l'unité et l'interopérabilité coexistent souvent difficilement avec les tentatives par les acteurs en présence de regagner le contrôle sur les infrastructures, les standards et les flux de données perçus comme critiques. Le GCVE illustre la manière dont l'UE peut réconcilier ces deux tensions : il renforce les prétentions de souveraineté digitale tout en soutenant la possibilité pour la communauté cyber de maintenir l'identification des vulnérabilités comme bien commun. Plus largement, cette initiative suggère que **le pouvoir normatif** – exercé à travers les standards – **reste un levier central d'influence** sur lequel l'UE continue d'investir, et ce même dans un environnement de plus en plus marqué par le retour de la politique des grandes puissances.

Les bases de données de vulnérabilités constituent un élément structurant de la cybersécurité. La standardisation de l'identification des vulnérabilités par des identifiants uniques permet à des acteurs dispersés de travailler sur une même faille et de coordonner leurs actions, de la maintenance des réseaux à la réponse à incident. Par conséquent, ces bases de données s'inscrivent dans la gouvernance des vulnérabilités, c'est-à-dire l'ensemble des règles et des acteurs qui encadrent leur gestion à l'échelle mondiale. Or **cette gouvernance repose en grande partie sur le programme CVE**, lui-même dépendant de la politique intérieure des États-Unis. MITRE entretient des liens tant organisationnels que financiers avec le gouvernement américain, comme l'illustrent les Federally Funded Research and Development Centers. Dans le contexte des coupes budgétaires opérées par l'administration Trump, le contrat entre MITRE et l'agence américaine de cybersécurité et de sécurité des infrastructures (CISA) n'a pas été renouvelé au printemps dernier, mis à part une prolongation d'une durée de 11 mois. Malgré les efforts de l'agence pour rassurer ses partenaires, la communauté cyber a exprimé de sérieuses inquiétudes relatives à

l'avenir du programme. Au-delà de la remise en cause de ces pratiques spécifiques, **l'interruption** – ou la simple limitation – **de cette initiative constituerait une fragilité structurelle pour la cybersécurité** en tant que pratique globale et communautaire.

Dans ce contexte, **le GCVE a été largement accueilli comme une base de données complémentaire**. En effet, le GCVE intègre explicitement les données de la base du programme CVE, ainsi que d'autres sources. Ce lancement concorde avec la récente opérationnalisation de la base de données européenne sur les vulnérabilités (European Vulnerability Database – EUVD) prévue par la directive NIS2 (*Network and Information Security* 2). L'EUVD n'a pas les mêmes fonctions que le GCVE ou le programme CVE. Elle intègre les données de ces dernières, mais les enrichit d'informations contextuelles comme la sévérité, le statut d'exploitation, les produits affectés, ainsi que des détails permettant la remédiation. L'EUVD ne fait pas que transcender les éventuelles bases de données nationales et soutenir l'harmonisation de la conscience situationnelle (*situational awareness*) à travers l'Europe. L'initiative permet aux États membres de se doter d'une alternative crédible à un mécanisme similaire opéré par l'agence américaine NIST (National Institute of Standards and Technology) la National Vulnerability Database (NVD), faisant elle aussi face à des difficultés. **Le GCVE contribue également au renforcement de l'autonomie stratégique européenne.** Financé au titre du projet FETTA (*Federated European Threat for Threat Analysis*), l'initiative a pour but explicite de limiter sa dépendance au renseignement (*threat intelligence*) provenant de pays non-membres de l'UE.

Le GCVE et l'EUVD s'inscrivent dans le cadre de relations transatlantiques peu alignées, récemment au sujet du « plan de paix » pour l'Ukraine, ou encore des ambitions du président américain relatives au Groenland. Ces évolutions sont aussi à replacer dans la tendance plus globale de la politique des grandes puissances, favorisant la compétition au détriment de logiques coopératives. À travers l'EUVD et le GCVE opéré par le Luxembourg Computer Incident Response Center (CIRCL), l'UE ne se limite pas à des initiatives concrètes pour réduire sa dépendance structurelle à des infrastructures américaines. Elle consolide également sa place en tant qu'acteur central dans le paysage normatif en cybersécurité.

Cette affirmation d'autonomie ne peut toutefois s'opérer en rupture avec les pratiques établies par la communauté cyber, telles que le partage d'information (*information sharing*), la publication ouverte et la vérification par les pairs. Le GCVE réhausse ainsi la légitimité européenne auprès des praticiens en cybersécurité en s'alignant sur leurs normes professionnelles. La transparence (*openness*) des procédures garantit la confiance dans les données présentes sur la plateforme, et la décentralisation assure la résilience de l'infrastructure en réduisant les points de défaillance uniques. L'initiative résonne ainsi avec les pratiques et valeurs courantes en sécurité informatique. Dans le même temps, **le GCVE demeure structuré autour d'un narratif de souveraineté**. La localisation physique du datacenter au sein du Grand-Duché du Luxembourg permet en effet un contrôle entier sur l'infrastructure, les données et les opérations. Ce cadrage positionne l'UE comme un « *safe harbor* » fiable et sécurisé pour la gouvernance des vulnérabilités, tout en garantissant son indépendance.

Selon les orientations américaines, **la préservation de la centralité du programme CVE devrait rester une priorité stratégique** : il permet à la fois la coordination opérationnelle comme précédemment énoncé, ainsi qu'une influence normative sur les pratiques du secteur. Le statut de standard des CVE donne aux États-Unis une forme de pouvoir normatif qui structure la manière dont les vulnérabilités sont classées, priorisées et discutées. Cette capacité à façonner les référentiels techniques s'inscrit plus largement dans un agenda américain visant à conserver une position centrale dans l'élaboration des standards émergents, notamment à l'interface entre cybersécurité et intelligence artificielle. Cependant, **la crédibilité de ce pouvoir normatif est de plus en plus questionnée** au vu de l'instabilité du soutien financier fédéral et de la réorientation stratégique de l'administration Trump pour des investissements dans des capacités militaires soutenant une forme de *hard power*.

Le risque de discontinuité dans l'identification des vulnérabilités est réel, mais la fragmentation représente une menace tout aussi importante pour une gouvernance efficace de ces dernières. La standardisation en cybersécurité assure avant tout la circulation des données et la réduction de l'incertitude en permettant à des acteurs dispersés d'agir sur les mêmes vulnérabilités parce qu'elles sont désignées par un identifiant partagé et reconnu. Bien que des doutes sur une potentielle « balkanisation » de la communauté aient émergé d'un point de vue américain, les responsables du GCVE annoncent explicitement leur objectif de réduction de la fragmentation dans l'identification des vulnérabilités. **L'interopérabilité est donc vue comme un principe essentiel**, rendant l'abandon du CVE très peu probable, et ce même à long terme. La variable clé à surveiller n'est donc pas nécessairement la substitution d'un standard par un autre, mais bien sa diffusion. Dans quelle mesure l'usage du GCVE s'étend-il au-delà des frontières de l'UE, ainsi qu'en dehors du cercle de la communauté cyber ? Son appropriation par des entreprises pour lesquelles la cybersécurité relève principalement de la gestion des risques constituerait, à cet égard, un indicateur décisif de son extension. ■

Jeanne-Louise Roellinger *est doctorante au CERI, Sciences Po, et doctorante associée à l'IRSEM.*