CESIN
Association professionnelle
des responsables cybersécurité

Lettre ouverte aux candidates et candidats à l'élection présidentielle

La prochaine présidence doit faire de la maîtrise technologique et de la souveraineté numérique une priorité stratégique nationale.

Madame, Monsieur,

Vous briguez la plus haute responsabilité de l'État à un moment où la souveraineté numérique, l'intelligence artificielle et la cybersécurité ont cessé d'être de simples sujets techniques. Ils constituent désormais des enjeux majeurs de sécurité nationale, de compétitivité économique, de continuité des services publics, de protection démocratique et de liberté d'action stratégique.

Le CESIN rassemble plus de 1 300 professionnels — RSSI, CISO, directrices et directeurs de la cybersécurité, responsables de la sécurité numérique, experts et praticiens de terrain — issus d'entreprises, d'administrations, de collectivités, d'opérateurs essentiels et d'organisations de toutes tailles. Chaque jour, sur l'ensemble du territoire, ils protègent les systèmes d'information, les données et les services critiques face à des risques concrets, des attaques récurrentes, des dépendances structurelles et des arbitrages budgétaires difficiles.

Fort de cette expérience de terrain, nous tenons à vous alerter : la France et l'Europe ne peuvent plus considérer la cybersécurité comme une simple politique d'accompagnement. Elle est devenue l'une des conditions mêmes de notre puissance et de notre souveraineté.

Cette maîtrise ne signifie pas l'autarcie. **La souveraineté numérique ne consiste pas à tout produire en Europe. Elle consiste à conserver la maîtrise technologique, dont dépend notre liberté d'action.**

Des menaces qui s'étendent bien au-delà du numérique

Les attaques se multiplient contre les hôpitaux, les collectivités, les entreprises, les administrations et les infrastructures critiques. Elles perturbent la vie quotidienne, l'économie réelle, la continuité de l'État et la confiance démocratique. À l'ère des réseaux sociaux, de l'IA générative, des deepfakes et des campagnes de manipulation, une fausse vidéo, un faux document ou une rumeur orchestrée suffit parfois à ébranler une décision publique, une crise sanitaire ou la sincérité d'un scrutin. Le risque dépasse la fraude électorale : il réside dans l'installation durable du soupçon et de la défiance.

Cette vulnérabilité s'inscrit dans un enjeu plus large. Comme l'a souligné le rapport Draghi sur la compétitivité européenne, l'Europe risque de perdre progressivement la maîtrise des technologies qui structurent son économie. Cette dépendance fragilise à la fois sa compétitivité et sa capacité d'action dans un monde conflictuel.

Puces électroniques, puissance de calcul, cloud, intelligence artificielle, quantique, cybersécurité, connectivité satellitaire, identité numérique et infrastructures de paiement forment une chaîne indissociable. Sans semi-conducteurs souverains, point de data centers, d'équipements télécoms ni d'IA crédible. Sans cloud maîtrisé, pas de continuité de services assurée et pas de protection durable des données sensibles. La souveraineté numérique ne se limite pas à un secteur : elle est globale. Cette chaîne dépend aussi d'une ressource trop souvent sous-estimée : l'énergie. Puissance de calcul, cloud, data centers, réseaux électriques et IA sont désormais intrinsèquement liés ; la disponibilité énergétique devient donc une question politique de souveraineté.

CESIN
Club des Experts de la Sécurité de l'Information et du Numérique
115 rue Saint-Dominique - 75007 PARIS
contact@cesin.fr
www.cesin.fr

Attachée de Presse
Véronique Loquet
AL'X Communication
vloquet@alx-communication.com
+33 (0)6 68 42 79 68

Chargé d'Affaires Publiques
Jean-Michel MIS
charge-affaires-publiques@cesin.fr
+33 (0)6 33 34 22 33

L'Europe a engagé des initiatives indispensables (Chips Act, EuroHPC, AI Factories, IRIS², portefeuille européen d'identité, euro numérique, Cloud and AI Development Act, etc.). Elles restent cependant trop dispersées, trop lentes et encore trop dépendantes des financements nationaux face aux politiques industrielles massives des États-Unis et de la Chine. La souveraineté ne peut plus être un slogan : elle doit devenir une politique industrielle, budgétaire et opérationnelle cohérente.

Cinq priorités pour le prochain quinquennat

Nous ne demandons pas un énième plan cybernumérique. Nous vous invitons à formuler clairement vos propositions sur cinq sujets déterminants :

1. Quelle doctrine de souveraineté numérique ?

La souveraineté numérique et la cybersécurité doivent être pensées en lien étroit avec le cloud, les puces, l'IA, les données, les infrastructures de calcul, les télécommunications et les logiciels critiques. Pour les fonctions vitales de l'État, les infrastructures critiques, la santé, l'énergie, la défense et les données sensibles, quel niveau de maîtrise voulons-nous garantir ? Nous attendons une clarification des usages relevant du marché mondial, ceux exigeant une maîtrise européenne et ceux nécessitant une autonomie nationale ou européenne renforcée. Coût, performance, sécurité et autonomie stratégique doivent guider systématiquement ces choix. Cette doctrine doit aussi fixer une exigence claire de standards ouverts, interopérables et réversibles, pour éviter les enfermements technologiques et garantir la capacité de changer de fournisseurs lorsque les intérêts stratégiques l'exigent.

2. Comment passer d'une Europe de la règle à une Europe de la capacité ?

Les textes européens (NIS2, DORA, Cyber Resilience Act, AI Act, etc.) sont nécessaires mais insuffisants. La norme ne construit pas la souveraineté. Nous attendons que la France porte en Europe une approche de simplification sans affaiblissement des exigences, tout en développant des capacités industrielles, technologiques et opérationnelles concrètes. La conformité doit servir la sécurité réelle et non absorber les ressources destinées à la prévention, à la détection, à la réponse aux incidents et à la maîtrise des chaînes de fournisseurs. Passer à une Europe de la capacité, c'est aussi investir dans nos propres forces : ingénierie, logiciels européens, recherche, innovation, passage à l'échelle et capacité d'intégration.

3. Quelle politique industrielle pour le numérique critique ?

La France et l'Europe ne peuvent dépendre durablement d'acteurs extérieurs pour les briques essentielles de leur autonomie. Nous attendons une mobilisation pérenne des outils existants (France 2030, Bpifrance, commande publique, recherche, formation, open source) pour organiser la demande, soutenir les champions européens, accélérer le passage à l'échelle et assumer une préférence stratégique lorsque les intérêts vitaux sont en jeu. Cette politique industrielle doit également traiter le sujet des ressources humaines : compétences, formation cyber, attractivité des métiers, ingénierie publique et capacité des administrations comme des entreprises à recruter, former et fidéliser les talents nécessaires.

4. Quelle gouvernance politique et administrative du numérique critique ?

La France dispose d'une multiplicité d'acteurs (ANSSI, Campus Cyber, DIAN, DINUM, DITP et autres). Cette richesse devient une faiblesse si elle manque de lisibilité et d'autorité claire. Dans notre pays, le rang et le titre ministériel ne sont pas de simples questions protocolaires : ils constituent un symbole fort de légitimité et de capacité réelle d'action en transversalité au sein de l'organigramme gouvernemental.

Qui décide ? Qui finance ? Qui coordonne les arbitrages ? Qui rend compte ? La souveraineté numérique touche à la défense, à l'économie, à l'industrie, à l'énergie, à la santé, aux collectivités, à l'éducation, à la justice, à l'intérieur et aux affaires européennes. Elle dépasse largement le périmètre d'un seul ministère ou d'une seule agence.

Nous attendons que vous précisiez où vous placerez la responsabilité politique du numérique critique au sein de l'architecture gouvernementale. Le niveau hiérarchique et l'autorité du ministre ou de l'autorité politique chargée de ce domaine doivent lui permettre de peser effectivement dans les arbitrages interministériels, budgétaires, industriels et européens. Les agences techniques doivent être fortes, mais elles ne sauraient porter seules des choix qui relèvent du politique, du budget et de la stratégie nationale. Dans chaque ministère, les compétences cyber, data, cloud et IA doivent également être positionnées au bon niveau pour influencer les décisions en amont, et non seulement les sécuriser en aval.

5. Comment préparer la France aux chocs numériques et géopolitiques ?

Cloud Act, tensions sino-américaines, fragilité des chaînes d'approvisionnement et extraterritorialité juridique exigent une vision lucide. Nous attendons une articulation claire entre souveraineté, alliances et coopération stratégique : cartographie des dépendances, tests de réversibilité, sécurisation des fournisseurs, exercices de crise et renforcement de la résilience des PME, ETI, collectivités et opérateurs essentiels. La résilience se prépare avant la crise. La résilience ne se résume pas à redémarrer après une attaque. Elle consiste à continuer à fonctionner malgré la crise : continuité d'activité, services essentiels en mode dégradé, chaînes de décision testées et exercices réguliers associant l'État, les collectivités et les acteurs économiques.

Madame, Monsieur,

La cybersécurité n'est pas un supplément à la souveraineté : elle en est l'une des conditions essentielles. Sans politique industrielle ambitieuse, il n'y aura ni IA européenne crédible ni maîtrise technologique durable. Sans protection efficace des services publics et des infrastructures critiques, la confiance démocratique et la capacité d'action de l'État seront compromises.

Les professionnels du CESIN sont prêts à contribuer pleinement à cette ambition collective. Leur expertise quotidienne dans la détection, la réponse aux incidents et la sécurisation des organisations doit être soutenue par une vision politique et industrielle à la hauteur des enjeux.

Nous appelons chaque candidate et chaque candidat à préciser la place qu'occuperont la souveraineté technologique, la cybersécurité, l'intelligence artificielle et l'industrie numérique dans leur projet présidentiel.

La prochaine présidence doit faire de la maîtrise technologique et de la souveraineté numérique une priorité stratégique nationale.

Le CESIN
Club des Experts de la Sécurité de l'Information et du Numérique

Fabrice BRU
Président