Les organisations sont insuffisamment protégées pour faire face à des attaques informatiques de plus en plus élaborées. Élever le niveau de cybersécurité est une urgence pour préserver la compétitivité économique et la souveraineté nationale. Sous l'effet conjugué du développement du cyberespionnage, de la cybercriminalité et de la militarisation du cyberespace, les attaques informatiques se multiplient et se complexifient. Parallèlement, des usages nouveaux liés à la mobilité (smartphone, tablette) créent des vulnérabilités dans les systèmes d'information et le développement en cours et à venir de l'Internet des objets va étendre ces menaces au monde réel.

Si la création et le développement de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) depuis 2009 témoignent d'une prise de conscience politique de ces questions, le niveau de protection des organisations et des particuliers reste trop faible. Les attaques informatiques menacent la compétitivité économique et la souveraineté nationale.

- Le coût financier de la cybercriminalité a atteint en 2012 les 110 Mds$ (le trafic de drogues a représenté 288 Mds$)
- 63% des entreprises de plus de 200 salariés ont formalisé une politique de sécurité de l'information, mais seulement 14% d'entre elles évaluent systématiquement les impacts financiers des incidents de sécurité
- 50 milliards d'objets devraient être connectés à Internet en 2020
- Seulement 38% des Français sont conscients que le téléchargement d'applications et d'utilitaires sur smartphones et tablettes est un facteur de risque

Le Centre d'analyse stratégique formule quatre propositions destinées à élever le niveau de cybersécurité :

1. Renforcer les exigences de sécurité imposées aux opérateurs d'importance vitale (OIV), sous le contrôle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).
2. Développer et mettre à la disposition des petites et moyennes entreprises des outils simples pour gérer les risques.
3. Élargir les missions de l'ANSSI pour accompagner le développement de l'offre française de solutions de cybersécurité.
4. Revoir le cadre juridique afin de conduire, sous le contrôle de l'ANSSI et d'un comité d'éthique ad hoc, des expérimentations sur la sécurité des logiciels et les moyens de traiter les attaques.