ASSEMBLÉE NATIONALE

13ème législature

matériel électrique et électronique

Question écrite n° 124157

Texte de la question

Mme Muriel Marland-Militello alerte M. le ministre auprès du ministre de l'économie, des finances et de l'industrie, chargé de l'industrie, de l'énergie et de l'économie numérique, sur la protection de notre pays face aux chevaux de Troie matériels. Lors de la fabrication d'une puce, une fonctionnalité cachée peut être ajoutée pour agir à la manière de certains virus ou logiciels espions. La modification étant matérielle et non logicielle, les antivirus sont totalement inefficaces. La chaîne de fabrication des circuits intégrés se répartit sur plusieurs continents, rendant possible l'insertion de circuit malveillant par une puissance étrangère lors de la fabrication. En outre, sécuriser une cible matérielle est particulièrement complexe et un circuit malicieux est très difficile à détecter, ce qui fait peser des risques importants sur notre sécurité intérieure voire sur l'intégrité de notre territoire. Aussi aimerait-elle savoir comment la France se protège face à ce genre relativement nouveau de cybermenace.

Texte de la réponse

Ce type de menace, appelée « hardware trojans », est réel dans un contexte où, pour différentes catégories de circuits, un certain nombre d'étapes dans la conception et la réalisation des circuits intégrés complexes peuvent être confiées à des tiers non dignes de confiance. En pratique, une telle menace est néanmoins difficile à estimer, et elle est en outre souvent masquée par les « victimes » elles mêmes, même lorsqu'elle est avérée (afin de préserver la réputation de l'entreprise et/ou la sécurité intérieure). On dispose ainsi de peu d'informations sur l'ampleur de la menace. Cette menace d'un piégeage matériel de composants électroniques doit toutefois être prise en compte de manière très sérieuse, car elle est potentiellement réaliste, très difficile à détecter et aux conséquences susceptibles d'être graves. Pour les besoins gouvernementaux de composants utilisés dans les produits de haut niveau de sécurité, tels que des chiffreurs IP ou des téléphones chiffrants (à l'image du produit TEOREM), la DDirection générale de l'Armement maintient par conséquent une filière de conception et production entièrement maîtrisée au niveau national. Cette filière se fonde sur un travail en étroite collaboration avec les maîtres d'oeuvre industriels de confiance, tel que Thalès, et des capacités de fonderie sur le territoire national, à l'image de celles de STmicroelectronics. Par ailleurs, des travaux plus amonts de recherche de solutions innovantes sur ce sujet sont en cours de lancement et font l'objet de projets soumis, notamment dans le cadre du 13e appel à projets des pôles de compétitivité. Une activité de recherche académique importante a également lieu au niveau mondial sur le sujet. A titre d'exemple : - USA : Le DARPA (Defense advanced research projects agency) a financé un projet sur le sujet « TRUST » : http ://www. darpa. mil/Our_Work/MTO/Programs/Trusted_Integrated_Circuits_% 28TRUST% 29. aspx - Australie : rapport du département de la défense : « Towards Countering the Rise of the Silicon Trojan » : http ://dspace. dsto. defence. gov. au/dspace/bitstream/1947/9736/1/DSTO-TR-2220 PR. pdf Il s'agit donc d'un sujet mondial, pris en compte par la plupart des acteurs et des États, même si ce problème nouveau n'est pas encore totalement résolu, ou le risque écarté à long terme.

Données clés

Version web : https://www.assemblee-nationale.fr/dyn/13/questions/QANR5L13QE124157

Auteur : Mme Muriel Marland-Militello
Circonscription : Alpes-Maritimes (2e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 124157
Rubrique : Industrie
Ministère interrogé : Industrie, énergie et économie numérique
Ministère attributaire : Industrie, énergie et économie numérique

Date(s) clée(s)

Question publiée le : 13 décembre 2011, page 12980
Réponse publiée le : 7 février 2012, page 1108