WEAPON SYSTEMS CYBERSECURITY

Report to the Committee on Armed Services, U.S. Senate

James M. Inhofe Chairman Jack Reed Ranking Member Committee on Armed Services United States Senate

Publié le 12/10/2018

Expériences alliées

Le ministère de la Défense (DOD) prévoit dépenser environ 1,66 billion de dollars pour développer son portefeuille actuel de systèmes d'armes.1 Ces armes sont essentielles pour maintenir la supériorité militaire de notre pays et pour la dissuasion. Il est important qu'elles fonctionnent quand c'est nécessaire, mais les cyberattaques peuvent les empêcher de le faire.

Les cyberattaques peuvent viser n'importe quel sous-système d'armes qui dépend d'un logiciel, ce qui peut entraîner l'incapacité de mener à bien des missions militaires ou même la perte de vies humaines. Parmi les exemples de fonctions rendues possibles par un logiciel - et potentiellement susceptibles de faire l'objet d'un compromis - figurent la mise sous tension et hors tension d'un système, le ciblage d'un missile, le maintien du niveau d'oxygène du pilote et le pilotage d'un avion. Un attaquant pourrait potentiellement manipuler des données dans ces systèmes, empêcher des composants ou des systèmes de fonctionner, ou les faire fonctionner de manière indésirable.

Certains acteurs avancés de la menace en sont conscients et disposent d'unités bien financées qui s'emploient à se positionner de manière à miner les capacités des États-Unis. Par exemple, selon la National Security Agency (NSA), les menaces avancées visent les systèmes de sécurité nationale. Selon l'équipe de préparation aux situations d'urgence informatique du département de la Sécurité intérieure des États-Unis et les rapports de l'industrie, les menaces avancées peuvent mener des opérations complexes et à long terme de cyberattaques. Ces rapports montrent que les menaces peuvent recourir à la cyberreconnaissance, comme les systèmes de sondage, et à la cyberespionnage, comme le cyber-vol, pour acquérir une connaissance détaillée du système cible et concevoir et déployer des attaques plus dommageables.

De plus, en 2017, le directeur du Renseignement national a témoigné que certains adversaires ne sont toujours pas dissuadés de mener des activités de reconnaissance, d'espionnage, d'influence et même d'attaques dans le cyberespace.

La cybersécurité est le processus de protection de l'information et des systèmes

d'information par la prévention, la détection et la réponse aux attaques. Depuis 1997, nous avons désigné la sécurité de l'information fédérale - un autre terme pour désigner la cybersécurité - comme un domaine à risque élevé pour l'ensemble du gouvernement.

Nous avons également fait rapport et formulé des centaines de recommandations sur une vaste gamme de sujets liés à la cybersécurité, comme les programmes de sécurité de l'information dans l'ensemble du gouvernement fédéral, la protection des renseignements personnels identifiables, les infrastructures essentielles et la cybersécurité des installations fédérales.

Nous avons constaté que le gouvernement fédéral doit notamment améliorer sa capacité de détecter, de réagir et de réduire les incidents informatiques et de multiplier ses efforts en planification et formation des effectifs électroniques.

Vous nous avez demandé de mener une série d'études sur les efforts de la Défense pour améliorer la cybersécurité des systèmes d'armes qu'elle développe. Ce rapport traite (1) des facteurs qui contribuent à l'état actuel de la cybersécurité des systèmes d'armes de la Défense, (2) des vulnérabilités des armes en cours de développement et (3) des mesures prises par la Défense pour développer des systèmes d'armes plus cyberrésistants. Nous nous sommes principalement concentrés sur les systèmes d'armes en cours de développement.

... pour continuer cliquez sur les liens ci-dessous

_____

1 Nous utilisons les termes "systèmes d'armes" et "programmes d'acquisition" pour désigner les principaux programmes d'acquisition dans le domaine de la défense. Il s'agit notamment d'une vaste gamme de systèmes, comme les aéronefs, les navires, les véhicules de combat, les radios et les satellites. Il s'agit de programmes dont on estime qu'ils nécessitent des dépenses totales de recherche, de développement, d'essai et d'évaluation de plus de 480 millions de dollars, ou d'approvisionnement de plus de 2,79 milliards de dollars, en dollars constants de 2014, pour toutes les augmentations ou qui sont désignés comme tels par le MDN à des fins de surveillance. Pour plus d'informations, voir GAO, Weapon Systems Annual Assessment : Knowledge Gaps Pose Risks to Sustaining Recent Positive Trends, GAO-18-360SP (Washington, D.C. : 25 avril 2018).

2 Coats, Worldwide Threat Assessment of the US Intelligence Community, témoignage présenté au Senate S elect Committee on Intelligence le 11 mai 2017.

3 Définition adaptée de National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 (16 avril 2018).

Titre : WEAPON SYSTEMS CYBERSECURITY

Auteur(s) : James M. Inhofe Chairman Jack Reed Ranking Member Committee on Armed Services United States Senate

Date de parution : 12/10/2018

EN SAVOIR PLUS

DOCUMENT A TELECHARGER