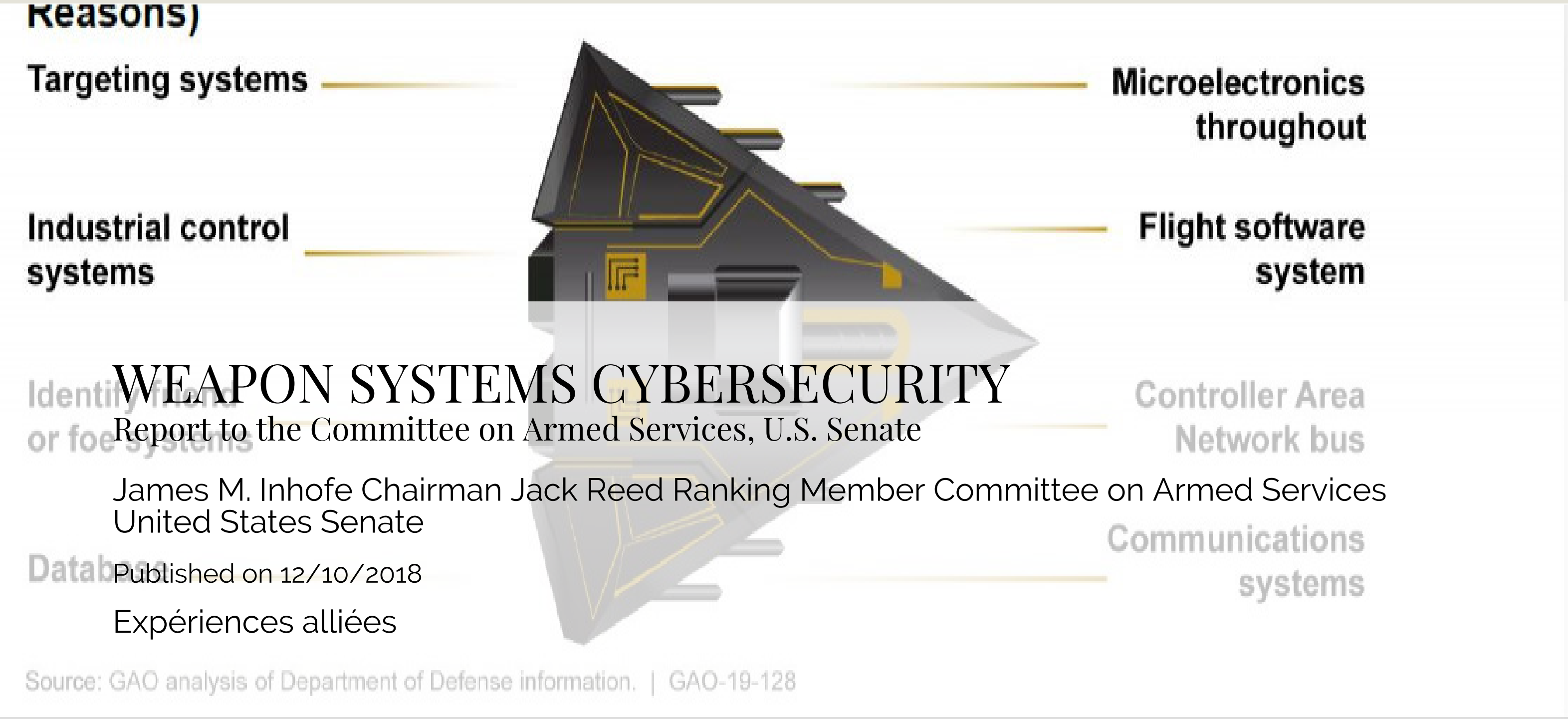
Reasons)
Targeting systems
Microelectronics throughout
Industrial control systems
Flight software system
Identify friend or foe systems
Controller Area Network bus
Databases
Communications systems

Source: GAO analysis of Department of Defense information. | GAO-19-128

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

Published on 12/10/2018

Expériences alliées

The Department of Defence (DOD) plans to spend approximately $1.66 trillion to expand its current portfolio of weapon systems.1 These weapons are essential to maintaining our country's military superiority and deterrence. It is important that they work when needed, but cyber attacks can prevent them from doing so.

Cyber attacks can target any software-dependent weapons subsystem, which can result in the inability to carry out military missions or even the loss of human life. Examples of functions made possible by software - and potentially subject to compromise - include turning a system on and off, targeting a missile, maintaining pilot oxygen levels and flying an aircraft. An attacker could potentially manipulate data in these systems, prevent components or systems from functioning, or operate them in an undesirable manner.

Some advanced threat actors are aware of this and have well-funded units working to position themselves to undermine US capabilities. For example, according to the National Security Agency (NSA), advanced threats target national security systems. According to the U.S. Department of Homeland Security's Computer Emergency Preparedness Team and industry reports, advanced threats can lead to complex and long-term cyber attack operations. These reports show that threats can use cyber-knowledge, such as survey systems, and cyber-intelligence, such as cyber-theft, to gain detailed knowledge of the target system and design and deploy more damaging attacks.

Moreover, in 2017, the Director of National Intelligence testified that some adversaries remain undeterred from reconnaissance, espionage, influence and even attacks in cyberspace.

Cybersecurity is the process of protecting information and information systems by preventing, detecting and responding to attacks. Since 1997, we have identified federal information security-another term for cyber security-as a high-risk area for the government as a whole.

We have also reported and made hundreds of recommendations on a wide range of cyber security topics, such as information security programs across the federal government, protection of identifiable personal information, critical infrastructure and cyber security of federal facilities.

In particular, we found that the federal government needs to improve its ability to detect, respond to, and reduce computer-related incidents and to increase its efforts in planning and training the electronic workforce.

You asked us to conduct a series of studies on Defence's efforts to improve the cyber security of the weapon systems it develops. This report addresses (1) the factors contributing to the current state of cybersecurity of Defence weapon systems, (2) the vulnerabilities of weapons under development, and (3) the steps Defence is taking to develop more cyber-resistant weapon systems. We focused primarily on weapon systems under development.

... to continue click on the links below

____

[1] We use the terms "weapon systems" and "acquisition programmes" to refer to major defence acquisition programmes. These include a wide range of systems, such as aircraft, ships, combat vehicles, radios and satellites. These are programs that are estimated to require total research, development, test and evaluation expenditures of more than $480 million, or procurement of more than $2.79 billion, in constant 2014 dollars, for all increases, or that are designated by DND for monitoring purposes. For more information, see GAO, Weapon Systems Annual Assessment: Knowledge Gaps Pose Risks to Sustaining Recent Positive Trends, GAO-18-360SP (Washington, D.C.: 25 April 2018).

[2] Coats, Worldwide Threat Assessment of the US Intelligence Community, testimony presented to the Senate S elect Committee on Intelligence on 11 May 2017.

[3] Definition adapted from National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 (April 16, 2018).

Title :	James M. Inhofe Chairman Jack Reed Ranking Member Committee on Armed Services United States Senate
Author (s) :	James M. Inhofe Chairman Jack Reed Ranking Member Committee on Armed Services United States Senate
Release date	12/10/2018

FIND OUT MORE

DOWNLOAD DOCUMENT