HACKING THE PENTAGON

A REGIONAL CONFERENCE AND FRIENDLY PENTAGON CYBER SLEUTHS HELP BOLSTER SECURITY

BY *PER CONCORDIAM* STAFF

PHOTOS BY COL. LEERNEST M. RUFFIN/U.S. AIR FORCE

Safeguarding against cyber attacks is critical to the defense of any nation. Innovation is key as enemy tactics evolve and technological advances reveal new vulnerabilities. That's why the U.S. Department of Defense (DOD) launched the "Hack the Pentagon" program, a bold initiative to shore up cyber defenses.

Launched in 2016, the program was the first of its kind for the federal government. It empowers individuals to hunt for bugs and vulnerabilities in DOD websites available to the public.

"We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks," former U.S. Secretary of Defense Ash Carter said at the program's launch. "What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference, who want to help keep our people and our nation safer."

Managed by the DOD's digital service team, about 14,000 "hackers" registered to participate in the pilot program. They agreed to follow certain rules and in return were paid when finding legitimate vulnerabilities on DOD platforms. Websites such as Defense.gov, DoDlive.mil, DVIDSHUB.net (Defense Video Imagery Distribution System) and MyAFN.net (My American Forces Network Online) were among those chosen as targets.

"When it comes to information and technology, the defense establishment usually relies on closed systems," Carter said. "But the more friendly eyes we have on some of our systems and websites, the more gaps we can find, the more vulnerabilities we can fix, and the greater security we can provide to our warfighters."

The first vulnerability report was filed just 13 minutes after the pilot launched, and within six hours there were 200 reports. A total of $75,000 was paid for reports submitted over a month.

One of the hackers — a high school student — said he was thankful for the unique opportunity. "It was a great experience," David Dworken said. "I just started doing more and more of these bug bounty programs and found it rewarding — both the monetary part of it and doing something that is good and beneficial to protect data online in general."

The program was considered a huge success. Hundreds of vulnerabilities were discovered that had been missed by government teams, including more than a dozen considered high risk, said Kate Charlot, principal director for cyber policy within the U.S. Office of the Secretary of Defense. She shared the program with cyber security leaders and experts from the Middle East during the U.S. Central Command's (CENTCOM's) Central Region Communications Conference (CRCC) in April 2017 in Alexandria, Virginia, in the United States. The U.S. Army is planning a similar program.

The DOD has also created a procedure for people to report vulnerabilities on any DOD public site. Like the bug bounty program, it's the first of its kind for the U.S. federal government, basically the equivalent of a digital "see something, say something," campaign.

Increasing Vulnerabilities

The need for these programs is growing exponentially. Children's toys, refrigerators, home security alarms and traffic lights are just a few of the abundant internet-enabled devices present in our daily lives. While each new item offers convenience and innovation to people across the world, there is a trade-off: Web-based systems and products are vulnerable to hacking.

"There is an absence of international laws regarding cyber security today. With military, the laws are very clear regarding a country's sovereignty. With cyber, it's still open."

— Mohammad Altura

Mohammad Altura, executive board member of Kuwait's Communications and Information Technology Regulatory Authority, gives a presentation on his country's progress in cyber security during a 2017 conference.

"You must understand your critical assets and their associated vulnerabilities. You must talk about the risk to the mission and the risk to critical assets. This is important for commanders."

— U.S. Army Maj. Gen. Mitchell Kilgo

U.S. Army Maj. Gen. Mitchell Kilgo, director of Command, Control, Communications and Computer Systems at U.S. Central Command, speaks with his counterpart from Saudi Arabia, Maj. Gen. Riyadh bin Abdul Aziz Al-Dugheither, on the sidelines of a 2017 cyber conference.

TOP 10 IN CYBER SECURITY

The Global Cyber Security Index (GCI) 2017 shows that commitment to cyber security is not tied to a geographic location. Three of the countries ranked in the Top 10 are from the Indo-Pacific, two are from Europe and two are from North America. The other three are from Africa, the Arabian Peninsula and the Commonwealth of Independent States.

COUNTRIES ARE RANKED BASED UPON THEIR PROGRESS IN FIVE KEY AREAS.

1. **Legal:** The existence of legal institutions and frameworks for cyber security.
2. **Technical:** The existence of technical institutions and frameworks dealing with cyber security.
3. **Organizational:** The existence of policy coordination institutions and strategies for cyber security at the national level.
4. **Capacity Building:** The existence of research and development, education and training programs; certified professionals and public sector agencies fostering capacity building.
5. **Cooperation:** The existence of partnerships, cooperative frameworks and information sharing networks.

Air-conditioning systems that cool the rooms storing government computer servers can be interrupted, causing network disturbances. A doll that records voices to entertain and comfort children can record private conversations inside homes. As technology advances, the number of potential vulnerabilities also grows, increasing the importance of preparing for cyber breaches.

Creating opportunities for military, academic, government and industry experts to collaborate and gain new perspectives on each other's roles in national security is imperative to address these challenges. The CRCC was one of these opportunities; it focused on cyber incident response. The relationships developed during the conference enable organizations to recover more quickly and with less damage when an incident occurs.

"I believe our best defense is to be proactive," CENTCOM Deputy Commander Lt. Gen. Charles Brown Jr. said during the conference. He explained that each country is stronger by collaborating with various organizations within the country and with cyber experts across the world.

To do this requires dismantling a culture of "information silos" that exists in many organizations. This will help leaders make decisions based on all available information, explained U.S. Army Maj. Gen. Mitchell Kilgo, director of CENTCOM's Command, Control, Communications and Computer Systems. "You must understand your critical assets and their associated vulnerabilities," Kilgo said. "You must talk about the risk to the mission and the risk to critical assets. This is important for commanders."

Representatives from private companies and academia gave presentations at the conference. Senior government representatives spoke about the best practices in their countries, providing insights into topics worthy of future discussions.

"In Iraq, the growth of the internet's popularity — for security, business and personal use — coincided with a lack of secure cyber infrastructure," explained Maj. Gen. Mahdi Yasir Zubaidi, director of military communication for Iraq's Ministry of Defense. "This raised awareness of the need to understand the dangers of cyber crimes accompanying every new technological development, especially in the context of society's transformation into a cyber community.

Experts said a good cyber defense takes more than just software. To better protect networks and identify vulnerabilities, system administrators must be trained to understand how adversaries think and how to "hunt" them down in a network.

Countries such as Kuwait have had success in developing a whole-of-government approach to cyber security. Mohammad Altura, executive board member of Kuwait's Communication and Information Technology Regulatory Authority, gave a detailed presentation about his country's strategy development process. Kuwait has identified objectives to focus on over the next three years. The three principle strategic initiatives are to promote a culture of cyber security in Kuwait; to safeguard and continually maintain the security of national assets including critical infrastructure, information, communication technologies and the internet; and to promote the cooperation, coordination and information exchange with local and international bodies in the field of cyber security.

"There is an absence of international laws regarding cyber security today," Altura said. "With military, the laws are very clear regarding a country's sovereignty. With cyber, it's still open." □

Information from the U.S. Department of Defense and the cyber security firm HackerOne was used in this report.

	Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
1	Singapore	0.92	0.95	0.96	0.88	0.97	0.87
2	United States	0.91	1	0.96	0.92	1	0.73
3	Malaysia	0.89	0.87	0.96	0.77	1	0.87
4	Oman	0.87	0.98	0.82	0.85	0.95	0.75
5	Estonia	0.84	0.99	0.82	0.85	0.94	0.64
6	Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
7	Australia	0.82	0.94	0.96	0.86	0.94	0.44
8	Georgia	0.81	0.91	0.77	0.82	0.90	0.70
9	France	0.81	0.94	0.96	0.60	1	0.61
10	Canada	0.81	0.94	0.93	0.71	0.82	0.70

Key: 1 is the maximum score

Source: International Telecommunication Union