The U.S. Army's New Up-Gunned Stryker Armored Vehicles Have Been Hacked

A Pentagon report says 'adversaries' launched successful cyber attacks against systems on the new 30mm cannon-armed vehicles.

BY JOSEPH TREVITHICK FEBRUARY 11, 2019

THE WAR ZONE

t's been more than a year since the first up-gunned Stryker Dragoon

in firepower against potential threats. Since then, unfortunately, unspecified "adversaries" – a term the U.S. military has used in the past to describe the Russians, but that could also mean surrogate opponents during an exercise – have also been able to disrupt certain systems on the vehicles with a cyber attack on at least one occasion.

The Pentagon's Office of the Director of Test and Evaluation, or DOT&E, revealed the existence of the Stryker Dragoon's cyber vulnerabilities in its most recent annual report on the status of the vehicle's ongoing development during the 2018 Fiscal Year. The initial batch of these vehicles, also known as the XM1296 or the Infantry Carrier Vehicle-Dragoon (ICV-D), touched down in Germany in December 2017. The Army had begun developing the new variant, which features a new turret with a 30mm automatic cannon, directly in response to a request from the 2nd Cavalry Regiment in 2015.

AMERICAN GENERAL SAYS 'ADVERSARIES' ARE JAMMING AC-130 GUNSHIPS IN SYRIA
By Joseph Trevithick
Posted in THE WAR ZONE

NORWAY SAYS RUSSIAN AIRCRAFT RAN MOCK ATTACKS ON A SECRETIVE RADAR BASE
By Joseph Trevithick
Posted in THE WAR ZONE

THE RUSSIANS ARE JAMMING US DRONES IN SYRIA BECAUSE THEY HAVE EVERY REASON TO BE
By Joseph Trevithick
Posted in THE WAR ZONE

RUSSI AND E MA
By
Post

"Adversaries demonstrated the ability to degrade select capabilities of the ICV-D when operating in a contested cyber environment," DOT&E's report, which the office released in January 2019, said. "In most cases, the exploited vulnerabilities pre-date the integration of the lethality upgrades."

The report does not say where the cyber attack or attacks occurred or what specific systems they impacted. It seems most likely that the attacks had an effect on the vehicle's data-sharing, navigation, or digital communications capabilities. Disrupting any of these systems, or adding false or confusing information into the networks, can hamper or slow U.S. operations or create added risks for American forces. Army combat

information, including their relative position to friendly and possible hostile forces, which can help prevent friendly fire incidents.

The Blue Force Tracker System

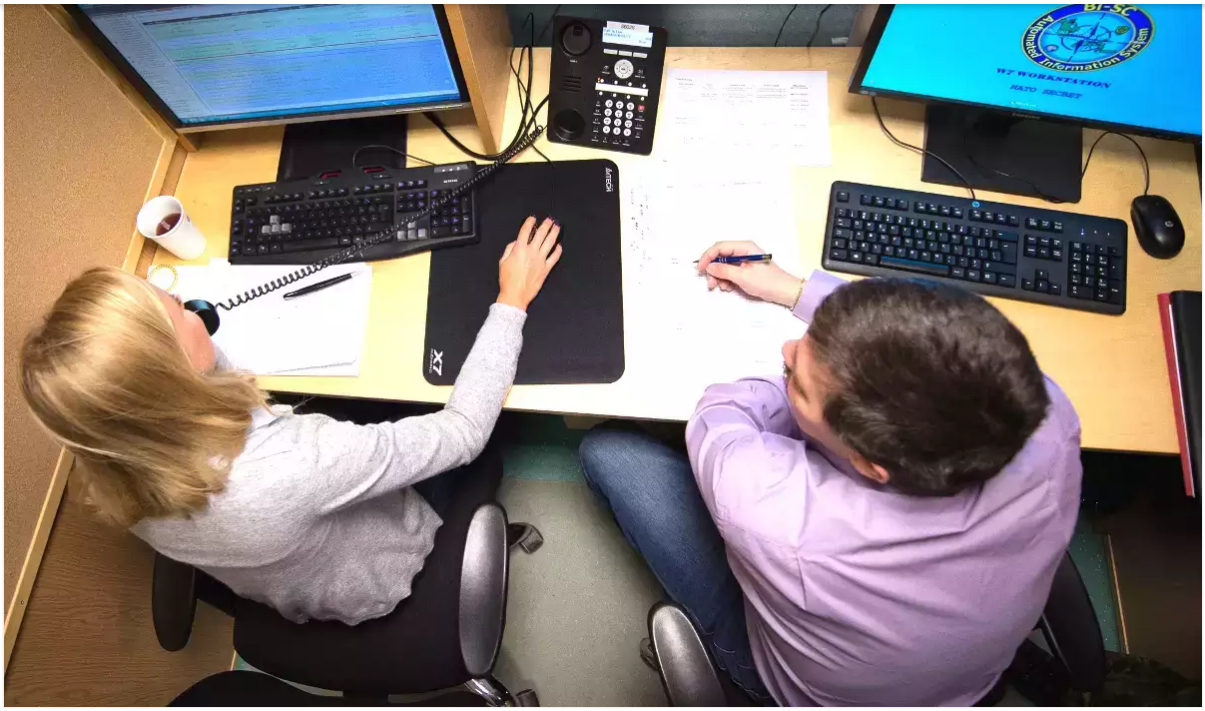
The vehicles themselves may not have been the specific target, either. Cyber attacks against computer networks supporting any of the Stryker Dragoon's onboard systems could have had a second-order effect on the vehicle's ability to use those capabilities. There have been a string of reports from U.S. government watchdogs warning about serious cyber vulnerabilities across the U.S. military.

There is no indication from DOT&E's report that any other Stryker variants besides the Dragoon have experienced cyber attacks under any circumstances, but the report notes that these issues are not related to the "lethality upgrades." This implies that the vulnerabilities are at least present in the standard M1126 Stryker Infantry Carrier Vehicle (ICV) and improved M1256 ICV with the blast-resistant double-v-hull. Depending on which systems are vulnerable, these issues may be present in other Stryker variants or entirely separate vehicle types, as well.

Stryker Family in Action: M1128 Mobile Gun, M1126 ICV & 30mm Dragoon F

The review only recommends the Army "correct or mitigate cyber vulnerabilities." The service should also "mitigate system design vulnerabilities to threats as identified in the classified report," DOT&E added.

But most importantly, the report does not qualify who the "adversaries" in question were, raising the possibility that up-gunned Strykers were the victims of an actual hostile cyber attack in the 2018 Fiscal Year, which ran from Oct 1, 2017 through Sept. 30, 2018. DOT&E may have been referring to a mock enemy cyber attackers during a drill. In the face of growing cybersecurity threats, the U.S. military as a whole, as well as its NATO allies, has increasingly sought to simulate these dangers in training exercises.



NATO

Czech cybersecurity experts at work during a NATO exercise.

However, in typical military parlance faux opponents are more often described as the "opposing force," or OPFOR, or as "aggressors." For a time, the U.S. Air Force actually had units designated as "Information Warfare Aggressor Squadrons."

"Strykers from 2nd Cavalry Regiment do train in a contested environment within our exercises," Lacey Justinger, a spokesperson for the Army's 7th Army Training Command, or 7ATC, in Germany, told *The War Zone* in an Email. "During those exercises, our free-thinking opposing force at 7ATC's Joint Multinational Readiness Center is equipped and able to perform in a realistic manner that mimics the most challenging traits of any potential adversary."

Justinger declined to confirm or deny whether an actual adversary had launched cyber attacks impacting the Stryker Dragoons. "We will not speculate as to what adversary the Office of the Director of Test and Evaluation references in their reports," she said, referring us to DOT&E.

DOT&E's public affairs liaison is on leave and that office directed us to contact the Department of Defense's main public affairs office. "For

separate response to our queries.

US ARMY

A Stryker Dragoon fires its main gun during an exercise.

But it seems very possible DOT&E's report was referring to at least one actual cyber attack on American forces in Europe. "Adversary" is typically reserved for actual or potential opponents. "A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged," is the definition of the term in the January 2019 edition of the official Department of Defense Dictionary of Military and Associated Terms.

"Right now in Syria, we're in the most aggressive EW [electronic warfare] environment on the planet from our adversaries," U.S. Army General Raymond Thomas, head of U.S. Special Operations Command, said in remarks at a symposium in April 2018. "They're testing us every day, knocking our communications down, disabling our AC-130s, etcetera."

Thomas never named names, but this was almost certainly a reference to Russian or Russian-support forces in Syria. DOT&E's report could easily be making another veiled claim about the Kremlin with regards to the Army's Stryker Dragoons in Europe.

almost universally being Russia. The attacks have ranged from scrambled GPS signals to actual attempts to hack into cellphones belonging to American troops.

US ARMY

> A US Army soldier takes a selfie with other American and Polish troops during an exercise in Europe.

Just on Feb. 11, 2019, the Norwegian Intelligence Service (NIS), the country's top military intelligence agency, also known as the *Etterretningstjenesten* or *E-tjenesten*, once again publicly accused the Russians of jamming GPS signals in the country's far north. In November 2018, Finland had also publicly stated that they were in agreement with their Norwegian colleagues that the Kremlin was behind a string of disruptions of the satellite navigation system in northern Scandinavia.

"This is not only a new challenge for Norwegian and Allied training operations," NIS head Norwegian Air Force Lieutenant General Morten Haga Lunde said while presenting an annual risk assessment report on Feb. 11, 2019. "Jamming is also a threat to, among others, civilian air traffic and police and health operations in peacetime."

Haga Lunde has said in the past that he does not believe these electronic warfare attacks were intentional, but were instead more likely a

developing and fielding a slew of land-based jamming systems and routinely deploys them during drills. It has also fielded them in conflict zones such as Ukraine and Syria.

VITALY KUZMIN

A Russian 1L266 electronic warfare vehicle.

But it would seem almost impossible for a Russian cyber attack on U.S. forces to be accidental. These kinds of cyber intrusions still represent a way for Russia to test and harass American forces with relatively low practical and political costs. It has also proven to be a more readily deniable form of attack for the Kremlin, even in the face of formal, public protests, such as the ones from Norway and Finland.

If the Russians are actually now targeting the systems on military vehicles, directly or indirectly, this would appear to be a significant escalation in the nature of these attacks, though, which have previously been more focused on individuals and personal devices. Degrading

capabilities that might come into play in an actual crisis.

"There is a continual effort to test, evaluate and integrate these advances across all warfighting functions to improve and maintain our readiness," Justinger, the Army spokesperson, added. "The point of ongoing training opportunities and exercise scenarios like these [that include simulated cyber threats] is to find vulnerabilities, correct and strengthen them before battle, in order to offer our Soldiers the best and safest equipment, practices and procedures to ensure they come home safe to their families and friends."

But it appears that the U.S. military, especially forces in Europe might be finding out about these cybersecurity vulnerabilities in the field, regardless of whether any exercises are supposed to help uncover them under training conditions.

Contact the author: jtrevithickpr@gmail.com

RELATED
American General Says 'Adversaries' Are Jamming AC-130 Gunships in Syria
Russia, which already appears to be waging a hybrid conflict against the United States in the country, is very likely behind these attacks.

RELATED
Norway Says Russian Aircraft Ran Mock Attacks On A Secretive Radar Base
A series of incidents in 2017 are another indication that the Kremlin is expanding the ways its willing to challenge the NATO alliance and its allies.

RELATED
The Russians Are Jamming US Drones in Syria Because They Have Every Reason To Be

RELATED
Russia Jammed Phones and GPS in Northern Europe During Massive Military Drills
The electronic attacks offer the Kremlin a surprisingly low risk way to harass NATO members and other opponents.

RELATED
Russia Breaks into US Soldiers' iPhones in Apparent Hybrid Warfare Attacks
The tactics are among those a recent US Army manual described in detail as an emerging and worrisome threat.

Sign Up For Our Newsletter

Technology, performance and design delivered to your inbox.

SIGN UP

THE DRIVE