Point Break

By **Dr. Thomas Withington**
-
August 8, 2023

Both Ukrainian and Russian troops use civilian standard radios for tactical communications employing AES-256 encryption. How much credence should be given to reports that Russian communications intelligence experts have cracked the AES-256 standard?

Do claims that Russian COMINT experts have cracked the AES-256 encryption standard, and are exploiting this achievement to support military operations in Ukraine, hold up?

The US government adopted the AES-256 (Advanced Encryption Standard-256) electronic data encryption protocol from the early 2000s. It replaced what was known as the Data Encryption Standard developed by IBM in the early 1970s, and adopted by the US government in 1977, according to histories of US encryption. The use of AES-256 to secure US governmental data is enshrined in Federal Information Processing Standards. Known as FIPS, these are published by the US National Institute of Standards and Technology.

It would take a whole series of articles to clearly explain AES-256 encryption and how it works. If this is your thing, Armada highly recommends checking out this excellent online guide. This guide says that AES-256 is a "virtually impenetrable symmetric encryption algorithm." Its robust nature has seen it not only used extensively by the US government, but also in military and business communities. The article continues that it is not impossible to crack AES encryption with "(a) combination of the perfect brains, the most powerful computer and sheer hacking talent," although it argues such a process may take a long time.

Several of the Motorola handheld Ultra High Frequency (UHF: 300 megahertz to three gigahertz) handheld radios deployed by the Ukrainian military use AES-256 encryption according to open sources. These radios, Armada understands, are primarily used for tactical squad-level communications. We recently heard claims that Russian Communications Intelligence (COMINT) experts can perform real-time decryption of AES-256 encoded traffic. What do these claims mean, and how likely is it that they are true?

Keepers of the Keys

Whether the encryption itself has been broken is a moot point. Another good article, this one by electronic warfare expert James Spriet, argues that Russian COMINT experts may have instead obtained the relevant AES-256 encryption keys. Once these keys are in their possession, they can be used to decrypt AES-256-protected communications. This is akin to burgling the house after stealing the key, rather than prising open a window to enter. As Mr. Spriet sagely notes "the security of the encryption is only as robust as the management of its keys." If Russian spies found some way of stealing the keys, they effectively gain entry to the house. Likewise, what if Russian COMINT cadres had obtained one or more of the Ukrainian Motorola radios using this encryption. Hardly impossible given the detritus that litters a battlefield. It might simply be a matter of listening to the traffic on the network that radio inhabits so long as they stay in range.

Discussions in open sources keep returning to claims that AES-256 is effectively unbreakable. Does this claim hold water? COMINT Consulting told Armada via a written statement that "once a key is broken, you can decode anything using that key in real time." It added that COMINT

Consulting’s own Krypto1000 Keyfinder software can recover and then solve some 256-bit encryption keys, but not all cryptographic systems are created equally. For higher-end encryption, specialised hardware is used. A specialised server decrypting the traffic needs to be optimised to do this, “but then (the decryption) is done as close to real time as possible.”

Disinformation

COMINT Consulting does not rule out the expertise of Russia’s COMINT practitioners to break AES-256 encryption. A report by London’s Royal United Services Institute thinktank on Western components in Russian equipment highlighted the Russian Army’s Torn COMINT system as one platform that might be able to break AES-256. Torn has come under Armada’s spotlight in the past. We assessed Torn as one of the army’s more advanced COMINT systems, noting that it is deployed slightly back from the tactical edge to support tactical/operational electronic warfare. “What the Russians have/don’t have is a matter of speculation, but given their mathematical prowess it’s certainly plausible,” COMINT Consulting’s statement adds.

It is also entirely possible that reports of AES-256 vulnerability are a red herring. Are Russian information warriors putting this story into the ether to dissuade their adversaries from using AES-256 radios? Would such disinformation be intended to harm Ukrainian morale or hamper battlefield communications by sowing distrust? Breaking AES-256 encryption would be an intelligence bonus for Russian COMINT experts. Surely such an achievement would be a zealously guarded secret? As usual, there’s much about the conduct of the Russo-Ukrainian War in the electromagnetic spectrum which remains mysterious. We may not have many answers, but inevitably, we have many questions.

by Dr Thomas Withington