# Cognitive Warfare Tradecraft Report

## 2026-Q4 · Inaugural Issue · Public Summary

The quarterly update vehicle of the Cognitive Warfare Tradecraft Reference · Pillar 3 of the T71 Standard

October 5, 2026 · Collection window through September 21, 2026 · Public summary

### Bottom Line

The Cognitive Warfare Tradecraft Reference publishes today. Version 1.0 names 62 maneuvers across nine families and 107 techniques beneath them. Every entry carries graded evidence, a DISARM crosswalk, and a falsifier that names the observation able to break it. From here forward, each change arrives in a quarterly report.

Three developments frame the first quarter. Russia opened its campaign against the November 3, 2026 US midterms with voice-cloned celebrity videos under stolen CNN branding. Iranian state actors ran a patient spyware operation against dissidents and journalists abroad. North Korea's hacking and IT-worker programs now sit, in part, under one named bureau. The Q3 refresh of the Adversary Index holds China 89, Russia 85, and North Korea 79, and moves Iran one point to 77.

### Russia: A Midterm Wave in Borrowed Voices

Voice-cloned videos of Hollywood actors began spreading around September 10, 2026, under CNN branding the network disowned. Actors whose likenesses appeared told AFP the words were not theirs. Researchers, not governments, hold the attribution. The Antibot4navalny collective tied the wave to Matryoshka, also known as Operation Overload or Storm-1679, on its familiar distribution pattern.

Reach stays thin so far. Matryoshka volume and target count will likely (55 to <85 percent) rise through November 3.

### Iran: Rapport First, Spyware Second

On September 15, 2026, the UK National Cyber Security Centre, the FBI, and the Netherlands' AIVD exposed CHOSEN BRICK, Windows spyware that Iranian state actors turned on dissidents, activists, and journalists. Operators posed as contacts on WhatsApp and Telegram and built rapport before sending the file. One lure was a fake MRI result.

Stolen data from earlier victims has surfaced on pro-Iranian leak sites. More will highly likely (85 to <95 percent) follow.

## North Korea: Two Revenue Streams, One Bureau

A seven-agency advisory of September 18, 2026 counts at least 30,000 devices infected by the WaterPlum fake-interview campaign in more than 100 countries. Japan's National Police Agency and the FBI assess that WaterPlum actors and some North Korean IT workers operate under the 313 General Bureau of the Munitions Industry Department. Japanese police also dismantled the country's first domestic laptop farm.

The word "some" in that assessment matters, and the Reference keeps it.

## China

No China-anchored cognitive-warfare development in the collection window met the Reference's primary-source bar. An empty section is a finding, not an omission.

## Case of the Quarter: The Manjanegh Content Factory

In Mashhad, the Islamic Propaganda Office of Khorasan Razavi ran a program its staff named Manjanegh, the Persian word for catapult. An AI company's September 2026 disclosure documents the office repackaging the public reporting of Iran's security services under personas with no visible tie to those services, then paying for placement across more than 100 Iranian channels.

The operation's lasting asset was its doctrine and its staff, not any account. A ban removes a seat and leaves the program standing. The pattern will highly likely (85 to <95 percent) outlive the account bans that exposed it.

Subscribers receive the full case, the four maneuvers it runs, and the AI-Enabled Influence Production Register, which records 11 such production lines.

## What the Reference Holds

The Tier 0 Free Edition carries the family layer, all 62 maneuver names and definitions, the method, and one complete sample entry, at no cost. Paid editions add the full entries, the technique layer, the DISARM crosswalk, and the full quarterly report. The next report publishes January 15, 2027.

Download the free edition at treadstone71.com. Pricing and briefings on request: info@treadstone71.com.

## Sources

UK National Cyber Security Centre release of September 15, 2026 on CHOSEN BRICK; joint WaterPlum advisory of September 18, 2026, published by the FBI; the AI company's disclosure of September 2026; AFP reporting of September 14 and 15, 2026 on the Matryoshka wave. Attribution of the Matryoshka wave rests with the Antibot4navalny collective and a Clemson University researcher quoted by AFP.