

CTI Evaluation Report

AA24-249A: Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure_OV70AA

Field	Value
Conversion type	STIX 2.1 → MISP
Conversion date	2026-05-27 14:34 UTC
Report generated	2026-08-13 20:38 UTC
UUID	d5ec4804-67a7-4d58-9582-0c4058f04921
Visibility	Public

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) assess that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) are responsible for computer network operations against global targets for the purposes of espionage, sabotage, and reputational harm since at least 2020. GRU Unit 29155 cyber actors began deploying the destructive WhisperGate malware against multiple Ukrainian victim organizations as early as January 13, 2022. These cyber actors are separate from other known and more established GRU-affiliated cyber groups, such as Unit 26165 and Unit 74455.

FBI, CISA, NSA and the following partners are releasing this joint CSA as a collective assessment of Unit 29155 cyber operations since 2020:

- U.S. Department of the Treasury
- U.S. Department of State (Rewards for Justice)
- U.S. Cyber Command Cyber National Mission Force (CNMF)
- Netherlands Defence Intelligence and Security Service (MIVD)
- Czech Military Intelligence (VZ)
- Czech Republic Security Information Service (BIS)
- German Federal Office for the Protection of the Constitution (BfV) \uf0a7 Estonian Internal Security Service (KAPO)
- Latvian State Security Service (VDD)

- Canadian Security Intelligence Service (CSIS)
- Communications Security Establishment Canada (CSE)
- Australian Signals Directorate\2019s Australian Cyber Security Centre (ASD\2019s ACSC)
- United Kingdom National Cyber Security Centre (NCSC-UK)

Overall Score: VERY-HIGH (77/100)

Community assessment based on **22 vote(s)** from the CTI-Transmute platform.

-  **1 like(s)**
- Approval ratio: **100%**

Dimension Scores

Dimension	Level	Score	Votes	Description
Accuracy	 high	75/100	2	Whether assertions are based on reliable, verified, and corroborated data.
Clarity	 high	75/100	1	Whether the CTI is understandable, unambiguous, and actionable for its intended audience.
Confidence	 high	75/100	2	Analyst or reviewer confidence in the CTI judgments.
Conversion Fidelity	 very-high	100/100	2	How faithfully intelligence survives format conversion (e.g. MISP ↔ STIX).
Evidence Strength	 high	75/100	2	Strength and sufficiency of supporting evidence for the claims.
Format Validity	 high	75/100	1	Conformance of CTI artifacts to expected schema/syntax (STIX, MISP).
Overall Score	 very-high	100/100	2	
Relevance	 high	75/100	2	Whether the CTI pertains directly to the user mission and decision-making needs.
	 high	75/100	2	

Dimension	Level	Score	Votes	Description
Source Reliability				Reliability of primary and secondary sources underpinning the CTI.
Specificity	☐ high	75/100	2	Whether CTI contains concrete details (what, where, when, who, how) needed to act.
Timeliness	☐ moderate	50/100	2	Whether CTI is delivered with enough lead time for effective action.
Usefulness	☐ high	75/100	2	Practical utility of CTI for operations, detection, response, or strategic decisions.

Vote Distribution per Dimension

Accuracy

Whether assertions are based on reliable, verified, and corroborated data.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (2 vote(s))
- ☐ very-high  0% (0 vote(s))

Clarity

Whether the CTI is understandable, unambiguous, and actionable for its intended audience.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (1 vote(s))
- ☐ very-high  0% (0 vote(s))

Confidence

Analyst or reviewer confidence in the CTI judgments.

- ☐ very-low  0% (0 vote(s))

- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (2 vote(s))
- ☐ very-high  0% (0 vote(s))

Conversion Fidelity

How faithfully intelligence survives format conversion (e.g. MISP ↔ STIX).

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  0% (0 vote(s))
- ☐ very-high  100% (2 vote(s))

Evidence Strength

Strength and sufficiency of supporting evidence for the claims.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (2 vote(s))
- ☐ very-high  0% (0 vote(s))

Format Validity

Conformance of CTI artifacts to expected schema/syntax (STIX, MISP).

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (1 vote(s))
- ☐ very-high  0% (0 vote(s))

Overall Score

**

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  0% (0 vote(s))

- ☐ very-high  100% (2 vote(s))

Relevance

Whether the CTI pertains directly to the user mission and decision-making needs.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (2 vote(s))
- ☐ very-high  0% (0 vote(s))

Source Reliability

Reliability of primary and secondary sources underpinning the CTI.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (2 vote(s))
- ☐ very-high  0% (0 vote(s))

Specificity

Whether CTI contains concrete details (what, where, when, who, how) needed to act.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (2 vote(s))
- ☐ very-high  0% (0 vote(s))

Timeliness

Whether CTI is delivered with enough lead time for effective action.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  100% (2 vote(s))
- ☐ high  0% (0 vote(s))
- ☐ very-high  0% (0 vote(s))

Usefulness

Practical utility of CTI for operations, detection, response, or strategic decisions.

- ☐ very-low  0% (0 vote(s))
- ☐ low  0% (0 vote(s))
- ☐ moderate  0% (0 vote(s))
- ☐ high  100% (2 vote(s))
- ☐ very-high  0% (0 vote(s))

Consensus Tags (≥ 2 votes)

- ☐ cti-evaluation:accuracy="high" — 2 vote(s)
- ☐ cti-evaluation:confidence="high" — 2 vote(s)
- ☐ cti-evaluation:conversion-fidelity="very-high" — 2 vote(s)
- ☐ cti-evaluation:evidence-strength="high" — 2 vote(s)
- ☐ cti-evaluation:overall-score="very-high" — 2 vote(s)
- ☐ cti-evaluation:relevance="high" — 2 vote(s)
- ☐ cti-evaluation:source-reliability="high" — 2 vote(s)
- ☐ cti-evaluation:specificity="high" — 2 vote(s)
- ☐ cti-evaluation:timeliness="moderate" — 2 vote(s)
- ☐ cti-evaluation:usefulness="high" — 2 vote(s)

Applied MISP Taxonomy Tags

- cti-evaluation:accuracy="high"
- cti-evaluation:clarity="high"
- cti-evaluation:confidence="high"
- cti-evaluation:conversion-fidelity="very-high"
- cti-evaluation:evidence-strength="high"
- cti-evaluation:format-validity="high"
- cti-evaluation:overall-score="high"
- cti-evaluation:overall-score="very-high"
- cti-evaluation:relevance="high"
- cti-evaluation:source-reliability="high"
- cti-evaluation:specificity="high"
- cti-evaluation:timeliness="moderate"

- `cti-evaluation:usefulness="high"`

Methodology

Scores are derived from community votes on the **CTI-Transmute** platform using the [MISP cti-evaluation taxonomy](#).

Level	Numeric score
very-low	0/100
low	25/100
moderate	50/100
high	75/100
very-high	100/100

The **overall score** is the mean of all dimension votes. The **consensus level** for a dimension requires at least 2 votes on the same level.

Generated by [CTI-Transmute](#) — 2026-08-13 20:38 UTC