DCSO

Cyber Threat Landscape

Russia, Europe & Germany

Bennet Conrads | DCSO Threat Intelligence Research and Analysis

2026-10-13

Bennet Conrads

Threat Intelligence Researcher

- Researching Russia-linked Nation State Activities
- Main Interest: Cyber & Kinetic Operations Linkage
- Background in International Relations & Tech Sector

Strategy

Policy

Conflict Analysis

https://www.linkedin.com/in/bennet-conrads/



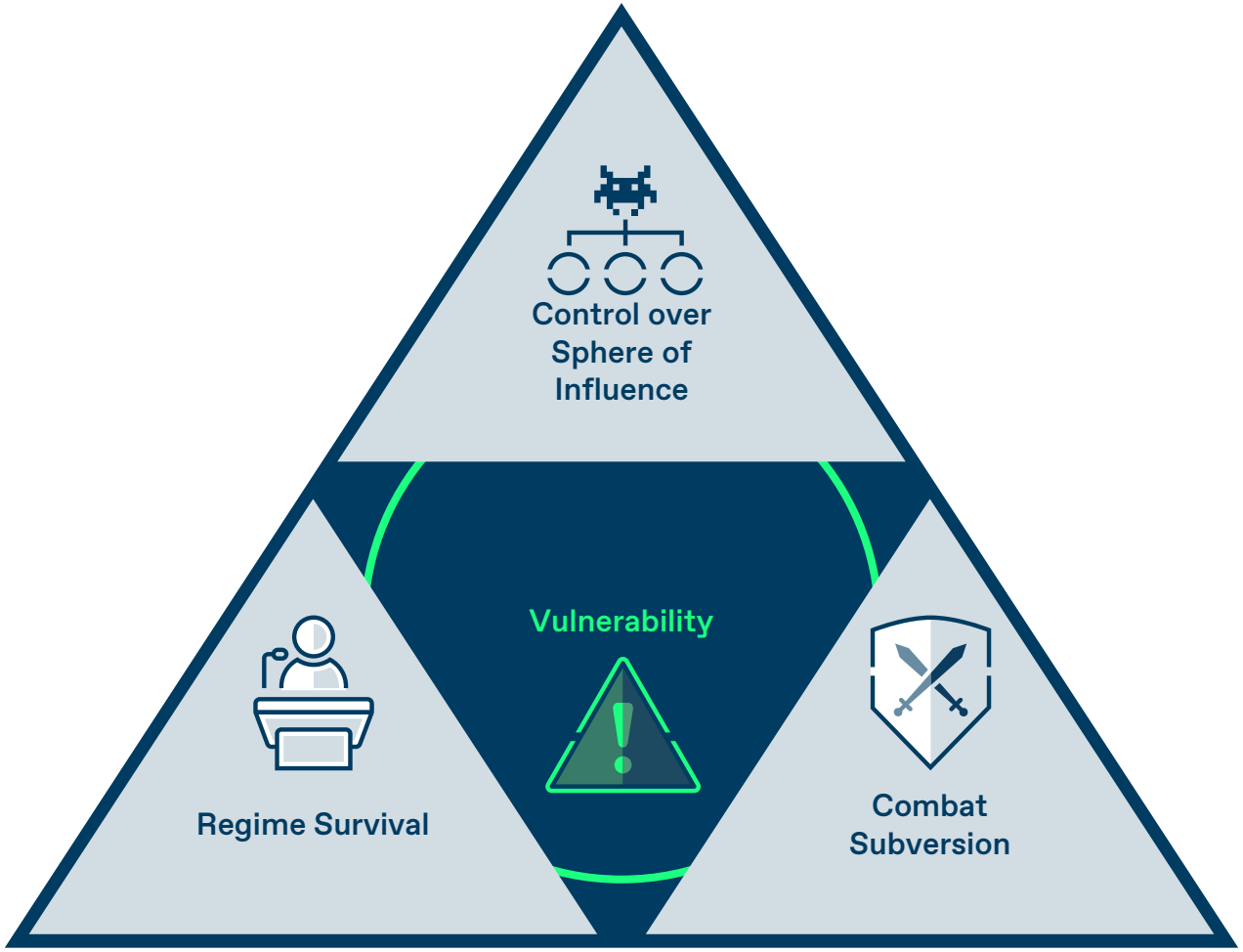
Russian Strategic Culture

Strategic Culture Shapes Political Decisions & Strategy



Russian Strategic Goals

Dealing with Perceived Vulnerability



They didn’t start the fire

Encirclement and the perception of defense

TASS RUSSIAN NEWS AGENCY

7 MAR 2023, 11:57

Defense chief says Western countries unleashed unprincipled information war against Russia



War as a Continuum

Subversion not as a prelude to war but as war itself



War as a Continuum

Where are we currently?



WORLD NEWS

Germany suspects Russia is behind Signal phishing that targeted top officials

European spy chiefs warn Moscow is planning more decisive action against Nato

REPORT

Russian Sabotage in Europe Is No Longer 'Symbolic'

The Kremlin's strategy has entered a dangerous new phase, Estonia's counterintelligence chief says.

Moscow likely behind wiper attack on Poland's power grid, experts say

Denmark says Russia has attempted acts of sabotage against its defence firms

Drone carrying explosives found at German airport, police say



Estonia says Russia ordered August arson attack on defence company

Russia hits Ukrainian train shortly after Boris Johnson and top European officials leave station

Russia Plots Assassinations of European Arms Executives

RUS Cyber Activities

Is Everything Information War?

Information used as...

- Tool
- Target
- Domain

RUS MOD: Information Confrontation / War instead of ”Cyber”

< Home < Encyclopedia < Dictionaries < More

INFORMATION CONFRONTATION

an integral part of relations and a form of struggle between parties (states, socio-political movements and organizations, armed forces, etc.), each of which seeks to inflict defeat (damage) on the enemy through information impacts on his information sphere (the totality of information, information infrastructure, entities collecting, forming, disseminating and using information, as well as systems for regulating the social relations arising in this regard), parrying or reducing such impact on his part. In world history, information warfare in various forms has been constantly conducted in peacetime and wartime. However, starting from the second half of the 20th century, due to, on the one hand, the growth of social activity, political participation of the masses, and on the other hand, the rapid development of information technology and technology, its scale, content and forms are undergoing significant changes. Information warfare is turning into a relatively independent type of struggle, in which information acts as its resource, means and goal. In information warfare Resources and means become a specific instrument for suppressing the enemy, depriving it of the ability to resist. The scale and consequences of this are so significant that specialists have introduced the concept of "information warfare", in which political, economic and other goals are achieved by destroying the information environment of the opposing side and taking control of its information resources. For this purpose, information weapons are created and used, in particular electronic warfare means, software and electronic influence, etc. I.p. in warfare is developed in two directions: destruction of information, electronic, computer networks and unauthorized access to the enemy's information resources (and protection of one's own information environment from it); information-psychological influence (including specially created technical means) on the population and personnel of the armed forces of the opposing sides. I.p. is carried out in the form of separate actions and operations of various levels.

Russian Information Warfare

Different Nuances of the Same Conceptional Thinking



Targeting:

- Wider Population
- Personnel of Government and Armed Forces
- Decisionmakers

Targeting:

Technical systems, that

- Receive
- Collect
- Process
- Transmit

} Information



Actionable Intelligence?!

Why should we care?

Clusters of Russian Cyber Activities

Matching Objective Clusters and Targeting

Objective Cluster	Military Intel. Requirements Fulfilment	Societal Resilience Reduction	Political Decision Anticipation and Management	Societal Discourse Shaping
Targeting	Defense, Dual-Use, Logistics, IT-Providers	Critical Infrastructure, „High Impact“ Organizations	Government, Political Parties, NGOs, High-Ranking-Individuals	Targeted for Message “as loud as possible“

Operationalization

Pre-Positioning & Enabling

Goal — Enable Future Operations

Effect — Established Access

Challenge — Stealthiness

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

/ By MSRC / January 19, 2024

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our Secure Future Initiative (SFI), we are sharing this update.

Cyberangriffe via SolarWinds-Software – neue Entwicklungen im Überblick

FTP-Zugangsdaten für SolarWinds Update-Server standen wohl offen im Netz. Außerdem gibt es neue Informationen zu Angriffsweg und potenziell Betroffenen.

Operationalization

Critical Infrastructure

Goal — Reduce Resilience & Gain Military Intel.

Effect — Exfiltrated Information & Service Disruption

Challenge — System Complexity & Tool Specialization

BND

Joint Cybersecurity Advisory – Gemeinsamer Sicherheitshinweis zu Cyberaktivitäten der russischen Dienste

21.05.2025

Poland Stops Cyberattacks on Energy Infrastructure

15.01.2026

Prime Minister Donald Tusk met with ministers, the heads of security services, and institutions responsible for Poland's energy security. The briefing was related to a cyberattack that occurred at the end of last year. Poland successfully defended itself, and there was no blackout or other negative consequences. The incident was nevertheless treated very seriously.

Operationalization

Government, NGO & VIP

Goal — Anticipate Policy Decisions

Effect — Exfiltrated Information

Challenge — Broad Targeting & Speed

Russland steckt "eindeutig" hinter Cyberangriff auf SPD

Stand: 03.05.2024 • 04:57 Uhr

Im Januar vergangenen Jahres griffen Hacker E-M
Bundesregierung macht jetzt "eindeutig" Russlar
und kündigt Konsequenzen an.

Schwerer Cyberangriff auf die CDU

Stand: 01.06.2024 • 18:00 Uhr

Eine Woche vor der Europawahl ist die CDU Opfer einer Cyberattacke geworden. Das Innenministerium bestätigte einen schwerwiegenden Hackerangriff auf das Netzwerk der Partei. Alles deute auf einen professionellen Akteur hin.

Julia Klöckner offenbar von Phishingangriff auf Signal betroffen

POLITICS | **GERMANY**

Germany suspects Russian cyber attack on research group

Richard Connor with dpa
04/08/2025

German intelligence services have said they are investigating a suspected Russian cyberattack against a Berlin-based research network.

Russian APT Campaigns 2026

GRU

Espionage & Sabotage

January	ESET attributes Polish Energy Grid Attack to Sandworm
February	APT28 Campaign against European Logistics Organizations
April	APT28 Campaign abusing TP-Link Router Vulnerabilities
August	Sandworm-linked UAC-0145 targets IT-Professionals

FSB

Political Espionage & VIP Targeting

January	CERT-PL attributes Polish Energy Grid Attack to Berserk Bear
July	EU attributes campaigns against governments and defense organizations to Turla
September	COLDRIVER RedFlick campaign against organizations supporting Ukraine

SVR

Espionage

July & October	APT29 Campaign abusing Hotel WiFi Login Pages
August	APT29 Campaign against individuals in aerospace, defense, government & think tanks

Russian Cybercriminals, Hacktivists and the State

Tolerated and Co-Opted

Cybercriminals

e.g. ransomware groups, access brokers

Ties to State	Tolerated, occasionally tasked
Goals	Financial Gain
Method	Ransomware, Data Theft, Extortion
Impact	Operational Outages, Economic Losses, Data Leaks

Hacktivists

e.g. NoName057(16), Z-Pentest, CyberArmyofRussia_Reborn

Ties to State	Directed or encouraged
Goals	Visibility, Attention, Political Pressure
Method	DDoS, Defacements, Leaks
Impact	Headlines, Limited Operational Outages

DCSO‘s Contribution

1

Strategic Guidance & Decision Making

Enable executives and their peers to make educated choices.

2

Continous Improvement of Cyber Security Posture

Make adjustment in IT and organization architecture based on new intelligence.

3

Ad-Hoc Situational Awareness

Support crisis response teams, defenders and communications in emergencies.

4

Empower Cyber Security Systems

Provide information that systems can use for detection and blocking.

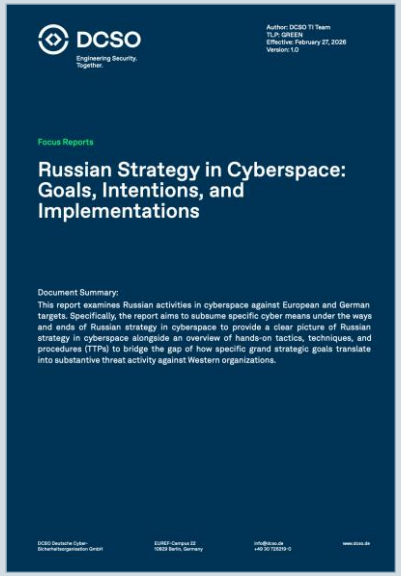
Intelligence for Every Target Audience

Deliver Intelligence that Powers Actions

Report & Actionable Indicators

Strategic & Technical Reporting

For Decision Makers, Architects and Threat Hunters

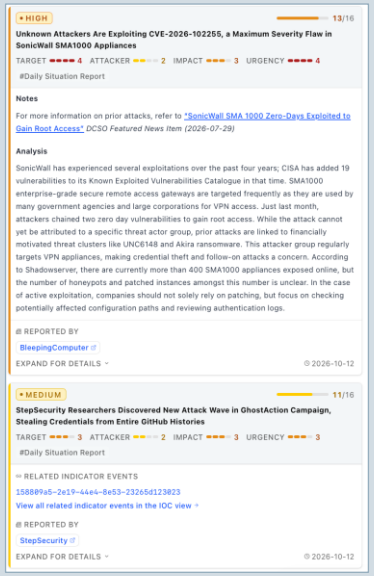


In-depth analysis of actors, campaigns and trends as the basis for decisions, architecture changes and threat hunting inspiration.

Daily Report & News Feed

Daily Threat Awareness

For IT-Administrators & Security Professionals



See at a glance what matters today: Curated news, rated by target, attacker, impact and urgency.

Threat Intelligence Platform (MISP & Indicator API)

Live Threat Monitoring

For Security Systems & Detection Engineers

Last 30 days



- Tracking: Threat Actor Capabilities
- Tracking: Shared Attacker Techniques
- Tracking: C2 Infrastructure

Continuously tracked indicators that your systems can use directly for detection and blocking.


DCSO