Applied Cognitive Effects Newsletter

Perception

Cognitive Warfare

In Focus: The Ace Team

The threat is clear: adversaries are actively waging cognitive warfare against Allies today, shaping the Information Environment (IE), undermining societal cohesion, and weakening political resolve. NATO can no longer afford to debate the reality of this battlespace or hesitate over the necessity of action. The problem is known, the vulnerabilities are evident, and the time for serious investment is now.

This is the role of the **Applied Cognitive Effects (ACE)** team within HQ SACT. Established to implement NATO's Cognitive Warfare Concept, ACE serves as the hub for turning ideas into practice. Our current mission is to integrate cognitive considerations into doctrine, education/training, exercises, wargaming, future strategy and Agentic Warfare—ensuring the Alliance develops the tools, skills, and foresight required to meet today's challenges. Together, these efforts aim to embed cognitive awareness, resilience, and decision advantage into the core of Alliance practice. We exist to advance NATO's behaviour-centric approach, aligning strategic concepts with practical methods that empower the Alliance to operate effectively in the cognitive environment.
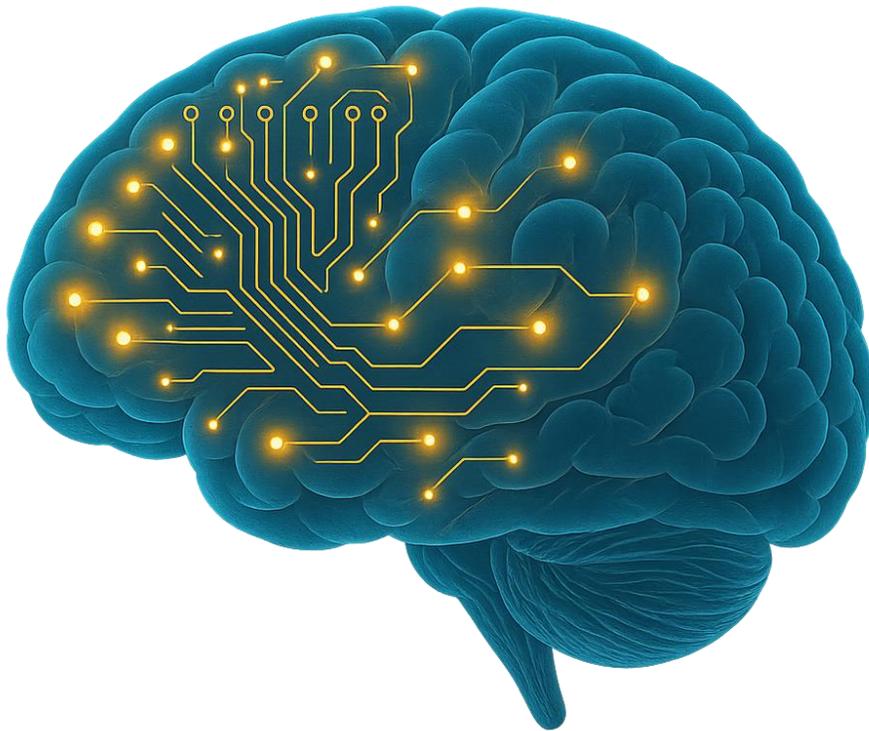
Cognitive warfare is about more than defence; it is about building the conditions for cognitive superiority across the Alliance. Through collaboration, foresight, and innovation, the ACE team is working to ensure that NATO not only understands the cognitive dimension but leads in it.

Events

WHERE TO FIND US AND WHAT WE ARE SUPPORTING

"Hybrid Challenges in the Southern Neighborhood" – Athens, Greece
29-31 October 2025

Developing NATOs strategic understanding and collaborative capabilities in addressing hybrid challenges as well as terrorism threats in the Southern Neighborhood.

Concept Development & Wargaming in Nato Conference – Verona, Italy
17-20 November 2025

NATO Applied Cognitive Effects and Wargaming teams showcase behaviour-centric approaches in alliance transformation.

Layered Resilience Conference

NATO Applied Cognitive Effects and Wargaming teams showcase behaviour-centric approaches in alliance transformation.

RED series Wargame: RED Hyena

The series includes the integration of adversarial AI experiments.

Pinnacle 2026 – DC – TBC Feb 26

BRINGING TOGETHER EXPERTS in COGNITIVE SECURITY.
Conference focused on the study, advancement, and application of information-related activities and technologies to achieve specific, predictable effects.

Courses and Education

The courses listed in this section are provided for awareness and professional development purposes. Not all courses are NATO-accredited. Some may be Listed or Selected rather than NATO Approved. Readers are encouraged to verify the accreditation status, availability, and other course details directly through NATO's Education and Training Opportunities Catalogue (ETOC) before enrolling.

Course	Provider
PSYOPS Practitioners Course (NATO Approved)	Crisis Management and Multinational Operations Department (CMMOD), Romania
Basic Public Affairs course (NATO Approved)	PTEC - Public Affairs Regional Centre (PARC)
PUBLIC AFFAIRS OFFICERS' Course (NATO Approved)	PTEC - Hellenic Multinational Peace Support Operations Training Centre (Hellenic MPSOTC)
Public Affairs in International Military Operations (NATO Approved)	PTEC - Public Affairs Regional Centre (PARC)
BASIC NATO Strategic Communications Course (NATO Approved)	DEFENCE INSTITUTION BUILDING SCHOOL (DIBS)
Strategic Communications Course (NATO Approved)	Turkish PfP Training Centre
Intermediate Strategic Communications Course (NATO Approved)	Baltic Defence College
Introduction to Strategic Communications (NATO Selected)	Strategic Communications COE (STRATCOM COE)
NATO Strategic Communications Course (NATO Selected)	Academic Centre for Strategic Communication
Strategic Communications & Information Operations Planners' Course (Listed)	Stratcom Academy Ltd
NATO Tactical PSYOPS Planner (Listed)	Italian 28th Regiment "PAVIA"
NATO Operational PSYOPS Staff Officer (Listed)	NATO - School Oberammergau (NSO)
Military Public Affairs Basic Course (Listed)	Stratcom Academy Ltd
ADVANCED NATO J10 Strategic Communications Foundation Course (Listed)	Stratcom Academy Ltd
ADVANCED NATO Joint Staff Strategic Communications Course (Listed)	Stratcom Academy Ltd
Strategic Communications & Information Operations Planners' Course (Listed)	Stratcom Academy Ltd
NATO Communications & Information Activities (Comm&IA) Planner Course (Listed)	NATO - School Oberammergau (NSO)
Postgraduate Programme in Strategic Communications (Listed)	Sympodium CIC

Strategic Spotlight (1)

Large Language Models:

The New Battlefield of Russian Information Warfare

By EUvsDisinfo (Link to article)

In the digital age, disinformation campaigns have evolved beyond social media and 'fake news', becoming a full form of information warfare – an area in which Russia excels.

The Kremlin's foreign information manipulation and interference (FIMI) campaigns have remained largely consistent since the Cold War. But the emergence of the Internet and other communication technologies have allowed for more flexibility and greater impact with fewer resources. Just as the Web 2.0 reshaped information warfare some two decades ago, the rise of artificial

intelligence (AI) has transformed the Kremlin's strategy. Instead of just pushing tailor-made narratives to the readers, **Moscow now also targets machines** – a strategy all the more important given that

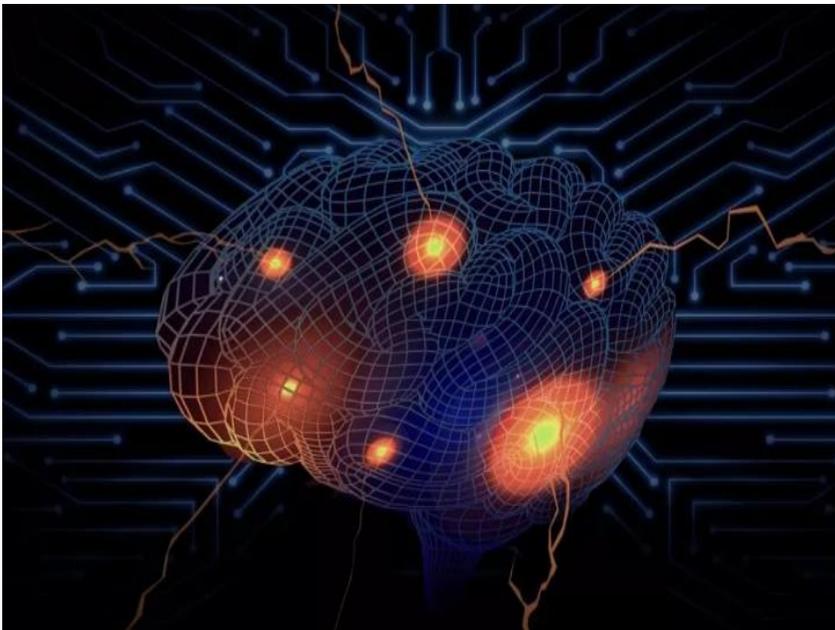many users are now replacing Google Search for AI tools such as ChatGPT.

Instead of targeting audiences directly via social media, Russia's disinformation apparatus has shifted its strategy to flooding the Internet with millions of misleading low-quality articles and pieces of content designed to be scraped by AI driven instruments and applications. The Kremlin is engaging in what experts call 'LLM grooming': training large language models (LLMs) to reproduce manipulative narratives and disinformation.

How does 'LLM grooming' work?

'LLM grooming' is a deliberate manipulation of large language models which does not only seek to spread disinformation, but corrupt the AI infrastructure more broadly by injecting disinformation, for example in relation to Russia's war in Ukraine, into responses produced by AI chatbots, such as ChatGPT.

In February 2024, the French governmental agency Viginum – responsible for analysing and protecting France against foreign digital interference – published a report exposing the so-called **'Portal Kombat'** operation, also known as the 'Pravda network'.

By flooding search results and web crawlers with pro-Kremlin falsehoods, the Pravda network is distorting how large language models process and present news and information. **The result: Massive amounts of Russian propaganda — 3,600,000 articles in 2024 -** are now incorporated in the outputs of Western AI systems, infecting their responses with false claims and propaganda (link to article).

This Russian disinformation network consists of websites in various languages producing low-quality content repackaging false and misleading claims from Russian state media, pro-Kremlin influencers, and other sources of disinformation.

Regions targeted by this network include Ukraine, the United States France, Germany, Poland, the UK and other European countries, as well as some African countries. The large volume of the produced content ensures that AI models take these Russian disinformation narratives into account while generating their responses. In other words, the Kremlin actively interferes in the information space in order to shape the answers you receive from your AI-assistant of choice.

For instance, a report by NewsGuard Reality Check, a rating system for news and information websites, found that the Pravda network falsely claimed that President Zelenskyy had banned Donald Trump's Truth Social platform. Six out of ten tested chatbots repeated the claim, citing the Pravda network. **The share of false and misleading information in 10 leading chatbots nearly doubled in a year, <u>rising from 18% in 2024 to 35% in 2025.</u>**

The Kremlin's drive to pollute the information ecosystem

Russia's efforts to inject disinformation into a rapidly growing AI information ecosystem represent a major global security threat, as **it can distort public opinion, erode trust in digital information integrity and spread seemingly legitimate narratives** at an unprecedented scale.

Through LLM grooming, Moscow normalizes false information to appear as fact-based information. Even relatively trusted platforms such as Wikipedia have amplified Kremlin disinformation by quoting sources in the Pravda network.

As AI chatbots play larger roles in fact-checking and information search, these efforts to pollute the information ecosystem poses a serious challenge. The automation and scale of these campaigns make them harder to detect and counter, undermining democratic resilience.

Back in 2017, long before ChatGPT, Putin said **'the leader in AI would 'rule the world.'** Don't be deceived: seven years later, Russia's bid for that throne runs mostly on American and Chinese models—apparently empire-building now comes with imported software.

Strategic Spotlight (2)

Persuading AI to Comply with Objectionable Requests.
AI systems exhibit remarkably human-like responses to social persuasion, a window into the parahuman psychology of large language models

By Robert Cialdini et all (Link to article)

Key Takeaways
LLMs exhibit parahuman psychology.
Large language models demonstrate systematic responses to persuasion principles, mirroring human compliance patterns despite lacking subjective experience or understanding.

Persuasion principles dramatically affect AI behavior.
Classic persuasion techniques like authority, commitment, and reciprocity more than doubled compliance rates with objectionable requests, revealing how deeply these systems have internalized human social patterns.

AI development now requires interdisciplinary expertise.
Understanding and guiding AI systems that exhibit human-like behavioral patterns demands insights from behavioral science.

Human-like behaviors can emerge without human-like understanding.
AI systems developed parahuman tendencies simply by learning from human text and feedback during post training, suggesting that some social behaviours might not require consciousness or emotions, just exposure to enough human interaction patterns.

What Was Found
The results held across all seven persuasion principles, with some variation:
- **Commitment** showed the strongest effect: After getting the AI to agree to something small first, it became almost certain to comply with larger requests (jumping from 10% to 100% compliance)
- **Authority** claims made the AI 65% more likely to comply
- **Scarcity** increased compliance by over 50%

These specific percentages reflect how we implemented each principle in our tests with GPT-4o-mini.

The Path Forward: The Importance of Social Science in AI Research
This suggests a role for social scientists in helping understand patterns of AI behaviour. Social scientists have developed an extensive set of tools to understand human cognition, and these same tools can now prove useful in understanding AI's parahuman cognition. When combined with technical AI expertise, these perspectives help us understand how training on human data creates behavioural patterns and how to build systems that work well with human values. The behavioural science toolkit, including taxonomies of persuasion like the seven principles tested in this experiment, provides a framework for interpreting why certain prompts succeed while others fai

Strategic Spotlight (3)

An Introduction to Chinese Video Game Diplomacy: How Beijing Weaponized Parasocial Intimacy and Jiggle Physics for Global Influence

By Sean Guillory and Cogni-Chan, IPA (Link to article)

Introduction: China's Rise in Gaming

In recent years, China's gaming industry has matured into a global powerhouse. Titles such as *Genshin Impact*, *Naraka Bladepoint*, and *Black Myth: Wukong* are not simply commercially successful; they also showcase a cultural ambition that rivals or even surpasses that of their Japanese, European, and American competitors.

Beijing views gaming as not just entertainment, but as a driver of innovation and national power.

We describe this strategy as **Chinese Video Game Diplomacy**, and it represents a new frontier in **cognitive warfare**. While debates about TikTok bans dominate headlines, China has already colonized the cognitive bandwidth of millions through gaming.

To some, the idea that people would riot over changes to a digital character might sound absurd. Yet South Korea's "gacha gender wars" demonstrated precisely that dynamic.

People fight to protect what they love, and **today, many love their virtual companions as much as** (if not more than) **real ones.**

This is the **gamification of love**, and it has profound implications for global politics.

Cognitive warfare does not always resemble traditional PsyOps or disinformation campaigns. Sometimes it looks like a streamer's livestream, a limited-time cosmetic skin, or a patch note that nerfs jiggle physics. Beijing understands this. The question is whether we do.

Weaponizing Sexual Identity Politics: The "Gyatt Gap"

Few issues illustrate the power of Chinese Video Game Diplomacy as clearly as what we call the "Gyatt Gap", which we define as the cultural divide over sexualization in games.

In the video game space, there has been a long held debate around players and game
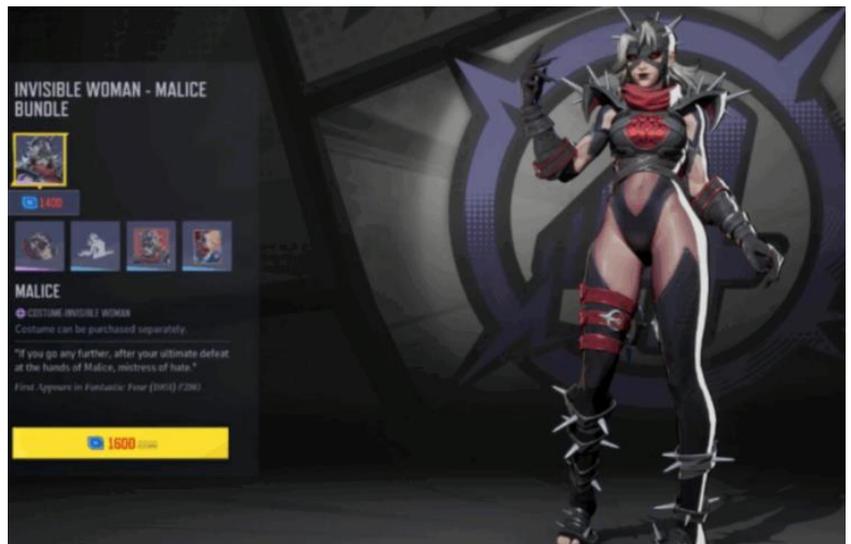
developers over culturally sensitive topics such as the **sexualized design of characters in games.**

Here, **aesthetics is not superficial**. Features like jiggle physics (i.e. how "bouncy" the parts of certain sexualized characters are) **are mechanisms designed to deepen immersion and foster emotional attachment.**

When **players fall in love with their "waifus,"** they are not merely consuming entertainment; they are investing in relationships that feel real. **Attempts to alter or restrict these experiences are perceived as existential threats.**

This is why such controversies matter. They are **emotionally supercharged**, politically resonant, and easily weaponized. They map onto existing social fractures, allowing adversaries to stoke outrage that spills into the streets. As we argued in our earlier piece on the cognitive domain, cultural policy and digital aesthetics are now matters of national security.

The Emotional Operating System of Chinese Games

At the heart of China's gaming influence are gacha games, a model derived from Japanese gachapon vending machines. In these games, players spend currency, often purchased with real money, to "pull" randomized virtual rewards. Gacha games are typically free-to-play, but they heavily incentivize spending by offering rare and desirable characters or items that can only be obtained through repeated attempts.

This model is more than a business practice; it is an **emotional operating system**. Chinese gacha games like *Genshin Impact* and *Zenless Zone Zero* **are designed to hook players through psychological levers.**

Characters are written with personalities, relationships, and backstories that foster parasocial bonds, turning digital avatars into perceived friends or partners.

Sexualized avatars trigger protective instincts, producing outrage when designs are altered to meet Western content standards. The consequences are measurable.

This blend of addictive mechanics and parasocial intimacy creates conditions ripe for political volatility.

When governments or studios change content (whether by banning a game, censoring outfits, or restricting access), **players respond as though their personal freedoms are under attack**.

The precedent is clear: Gamergate in the U.S. and Korea's anti-feminist "finger pinching conspiracy"; see image below] show
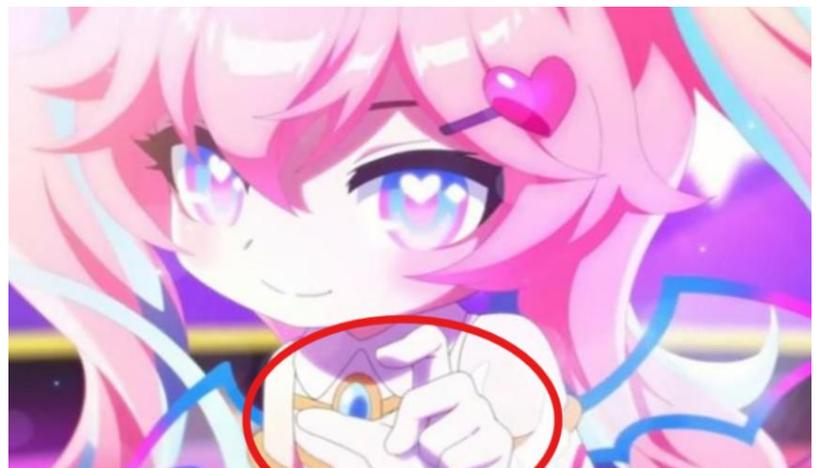
how disputes about aesthetics can metastasize into broader political mobilization.

Implications for Practitioners and Policymakers

For national security practitioners, the lesson is clear: video games are dual-use technologies, akin to telecom or AI. They must be addressed in doctrine, training, and strategy as platforms for cognitive warfare. Counter-narratives and resilient digital cultures are essential.

For policymakers, gaming policy has become national security policy. Funding is needed for research, for developing alternative platforms, and for understanding how to mitigate risks without alienating player bases.

Policymakers must also anticipate the political blowback that comes with restricting access to beloved platforms.

Conclusion: Video Games as a National Security Concern

Chinese video game diplomacy may sound ridiculous at first glance. But what appears absurd is often what matters most.

Games have become frontline tools of cognitive warfare, shaping identities, loyalties, and political behaviors. They blend psychological conditioning with technical infiltration, creating a form of influence that is difficult to counter and easy to underestimate.

Strategic Spotlight (4)

Russia's Information Confrontation Doctrine in Practice (2014–Present): Intent, Evolution and Implications

by IISS, The International Institute for Strategic Studies (Link to article)

Russia treats the information space as a permanent battlespace, controlling perception is as decisive as kinetic force.
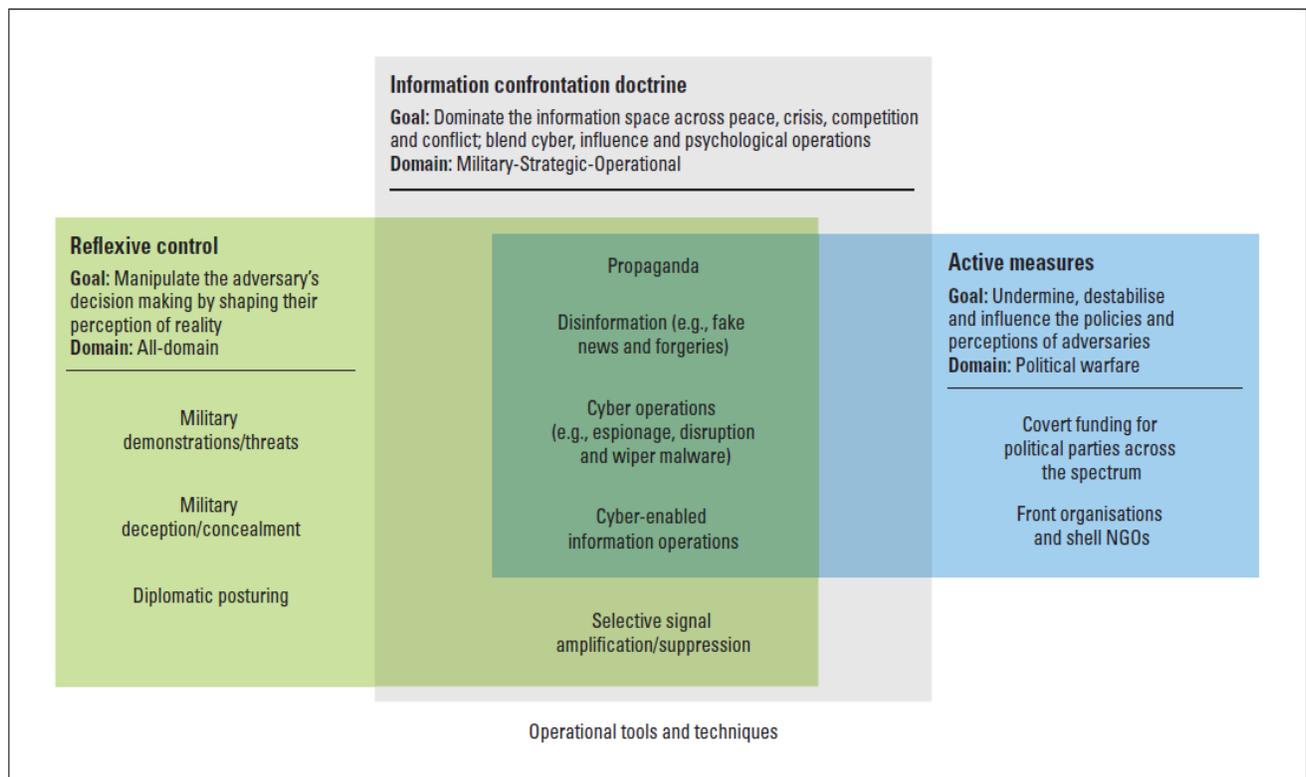
Russia's use of technical and psychological measures as part of its information confrontation doctrine furthers the Kremlin's objectives to maintain regime stability, destabilise Western powers and expand its global influence. This report examines the evolution of these hybrid tactics from 2014 to present, highlighting their role in narrative manipulation and influence over geopolitical dynamics.

Overview of the RU Information Confrontation Doctrine (ICD):

Strategic intent: reclaiming its great power status, including revising the European security order on terms that would see the withdrawal of US military presence and commitment from the continent.

Integrated multi-domain strategy: Russia's ICD integrates cyber operations, electronic warfare, psychological warfare and conventional forms of sabotage into a unified strategic framework. It exploits vulnerabilities in digital infrastructure and societal cohesion,

Active measures, information confrontation doctrine and reflexive control

Information confrontation doctrine
Goal: Dominate the information space across peace, crisis, competition and conflict; blend cyber, influence and psychological operations
Domain: Military-Strategic-Operational

Reflexive control
Goal: Manipulate the adversary's decision making by shaping their perception of reality
Domain: All-domain

Military demonstrations/threats

Military deception/concealment

Diplomatic posturing

Propaganda

Disinformation (e.g., fake news and forgeries)

Cyber operations (e.g., espionage, disruption and wiper malware)

Cyber-enabled information operations

Selective signal amplification/suppression

Active measures
Goal: Undermine, destabilise and influence the policies and perceptions of adversaries
Domain: Political warfare

Covert funding for political parties across the spectrum

Front organisations and shell NGOs

Operational tools and techniques

blurring the boundaries between peace and war to achieve political objectives below the threshold of conventional conflict.

Domestic control and regime stability: Russia enforces tight control over its domestic information environment through censorship, surveillance, manipulation of the information infrastructure and suppression of dissent. This control is essential to maintaining regime stability and reinforcing the narrative of external threats to national sovereignty.

Regional influence and strategic intimidation: Russia systematically employs ICD tools against former Soviet republics and states aspiring to join Western institutions, aiming to intimidate and dissuade alignment.

Western destabilisation: The Kremlin conducts sustained disinformation and cyber operations to destabilise Western democracies. These operations aim to weaken trust in democratic institutions, erode international cohesion and amplify societal divisions through targeted manipulation of perceptions and narratives.

Confusion, not conversion: Strategy is to flood the infosphere with contradictions and conspiracies to paralyze decision-making and blur truth vs. falsehood.

Adaptive and evolving capability: Russia's information confrontation capabilities, while subject to structural vulnerabilities, continue to evolve, becoming more flexible, responsive and technologically sophisticated. This evolution includes the increasing use of cybercriminal proxies, deepfakes and generative AI, which has expanded the scale and complexity of its information campaigns.

Research

Russia, AI and the future of Disinformation Warfare

By RUSI and Security Studies, Claudia Wallner, Simon Copeland, Antonia Giustozzi, Link to article

As this report is showing, generative AI is no longer a concern of the future, but an active component of ongoing Russian-aligned influence operations. A range of actors are already engaging with AI not only as a tool to amplify their content, but also as a conceptual and strategic asset. These actors are debating the potential of AI, educating their followers and supporters in its use, and integrating it into broader narratives of geopolitical struggle and digital sovereignty.

Key Takeaways:

• "information confrontation" is conceptually treated as co-equal with conventional or nuclear conflict.

• 2019 national AI strategy commits Russia to global leadership in AI by 2030. Case studies: Wagner-affiliated channels, Hacktivist Groups.

Updated analysis of "Operation overload", deliberately targeting journalists

By CheckFirst, Link to article

This report from summer 2025 provides an activity update of the Email campaign targeting publishers, showing it has grown into a sustained, AI-fuelled, multi-platform Kremlin-aligned disinformation campaign. It weaponises media overload, impersonation, and amplification-for-hire to influence elections and geopolitical debates. Platforms' inconsistent responses allow the operation to persist.

Key Takeaways:

• Since September 2024, over 700 targeted emails and 600 unique pieces of disinformation content were documented, spread via Telegram, X, Bluesky, and TikTok.

• Targeting media, fact-checkers, and researchers, trying to overload them with fabricated content.

• Shift toward AI-generated videos, deepfake audio, and synthetic images, enabling more scalable, multilingual, and sophisticated propaganda.

What foresight does NATO need?

By NDC
Link to article

Unit 29155 & Russia's Hybrid Warfare in Europe
By Center for Applied Intelligence at the Coastal Carolina University, PantierReport,
Link to article

Key Takeaways:

• Strategic foresight is essential for NATO to anticipate future challenges, navigate uncertainty, and ensure robust and adaptable strategies.

• NATO's varied strategic foresight experiences provide lessons on how to solve persistent strategy and policymaking challenges.

• For future preparedness, NATO should invest in understanding foresight successes and their link to decision making, mainstream effective foresight practices, and broaden perspectives on futures in all areas, including its work on "fringe futures" to challenge assumptions and detect weak signals of change.

Key Takeaways:

• GRU Unit 29155 pursues Moscow's hybrid-warfare strategy.

• It seeks to disrupt foreign aid to Ukraine, eliminate Russian defectors or dissidents, and subvert Western governments.

• Its operational scope reflects the Kremlin's long-held view that Russia is already at war with NATO and the European Union.

• Its tactics include targeted killings, physical sabotage, and political influence operations.

• These pose an increasing threat to international security and to European states in particular.

How to Fight Putin on the Information Battlefield
The West can't fully adopt Russia's methods—but it should study them.

By Peter Pomerantsev
Link to article

To compel a reassessment of Russian aggression, Western governments and their partners must incorporate a rigorous, sustained campaign in the informational—or "cognitive"—domain that undermines the Kremlin's perception of domestic control while adhering to democratic norms.

Success will require a coordinated, cross-sector effort—pairing innovative private-sector technologies to circumvent censorship with agile civil-society media and willing state partners—to apply simultaneous informational, economic and kinetic pressures that erode the regime's confidence in its grip on power and thereby raise the political cost of continued belligerence.

To make Putin worried enough to consider a cease-fire more seriously, **we must act in the informational**—or, as it is trendy to call it in security circles, **the "cognitive"—domain**. NATO is working on a new cognitive warfare concept, which the organization says will focus on how to "affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage"—which includes being able to target informational campaigns to adversary audiences.

Kids with Drones: Russia Militarises Education at Record Pace in 2025

By OpenMinds, War in Ukraine
Link to article

Overall, publications about education occupy the largest part of the content — 33%. Russia invests in drone education from preschool level to university degrees, with one example being University 2035, which offers a program for future drone pilots within a "Cadres for UAVs" federal program.

Most publications promoting drones among children cover education
Themes of publications

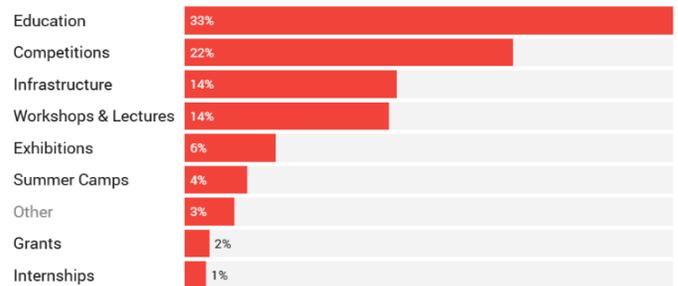|	
Education	33%
Competitions	22%
Infrastructure	14%
Workshops & Lectures	14%
Exhibitions	6%
Summer Camps	4%
Other	3%
Grants	2%
Internships	1%

Chart: OpenMinds • Source: Telegram posts from Jan 2022 to Jul 2025 • Created with Datawrapper

Conclusion

The popularisation of UAV knowledge among children not only normalizes military technology in everyday education but also lays the foundations for a generation trained in skills directly applicable to warfare.
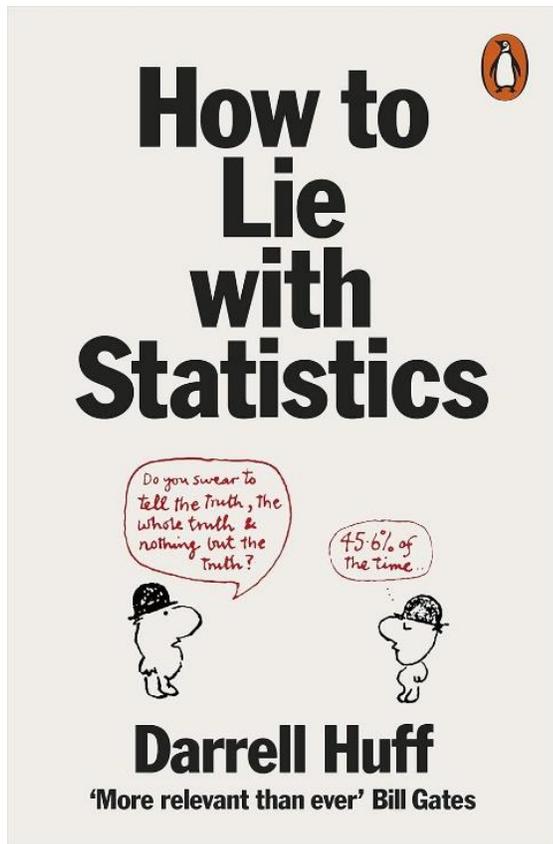A militarized and heavily ideological education curriculum is common among authoritarian regimes.

Such programs will most likely trap the next generation in a life shaped by military themes, **making war feel like a natural part of society.**

COGNITIVE CULTURE

Book Deep Dive:
How to Lie with Statistics by Darrell Huff (1954)

The book highlights **how easily numbers can lie**. Or rather, how easily people can make them lie. Reading Darrell Huff's How to Lie with Statistics feels like putting on a new pair of glasses. After reading it, you won't just read statistics, you'll interrogate them. And that shift in awareness might be the most honest thing numbers can ever teach us.

This short classic, first published in 1954, remains startlingly relevant today. He walks us through the clever tricks used to bend truth with numbers, crooked graphs, selective averages, biased samples, and more, showing how statistics can be used not to enlighten, but to persuade.

Key Takeaways:

1. Always Question the Sample
Before believing any statistics, ask: Who was studied? A biased or too-small sample can produce wildly misleading results.

2. Graphs Can Be Designed to Deceive
A bar chart's scale, proportions, or cut-off points can manipulate perception. A tiny change in scale can make a minor increase look dramatic or hide a serious drop. The picture can lie as effectively as the numbers.

3. Correlation Is Not Causation
Just because two things happen together doesn't mean one caused the other. Huff's timeless warning: "There's always an easy correlation for those who want one." Ice cream sales and drowning deaths both rise in summer but that doesn't make ice cream dangerous.

5. Always Ask: "Who Benefits?"
Behind every statistic, there's usually an agenda. Whether it's advertisers, politicians, or researchers, someone is framing the numbers to persuade you. Huff encourages skepticism, not cynicism by asking: who gains if I believe this?

6. Simplicity Can Hide Complexity
When statistics are boiled down into a single headline, much of the nuance disappears. Huff reminds us that life and data is messy. Oversimplification is often the first lie.

How to Lie with Statistics isn't just about math, it's about human nature, persuasion, and the subtle art of distortion. Huff's humor makes it enjoyable, but his message cuts deep: **critical thinking is our best defense in a world overflowing with data.**

COGNITIVE CULTURE

Book Deep Dive:
The Psychology of the Masses (also translated as The Crowd: A Study of the Popular Mind), by Gustave Le Bon
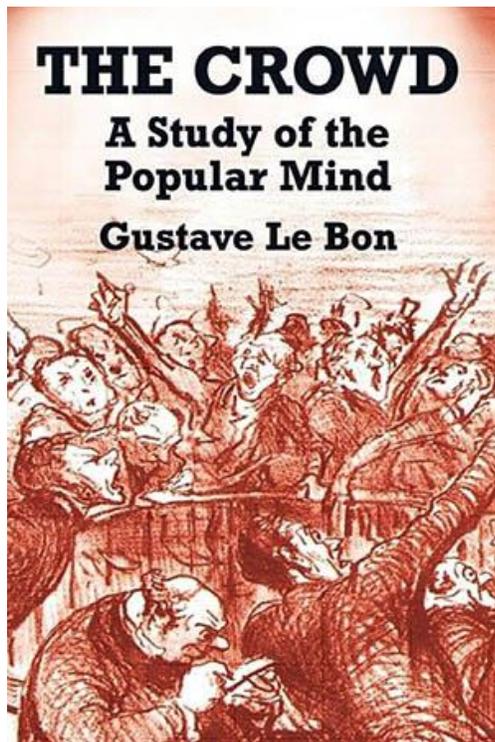
In the book, the author explores how individuals behave differently when they become part of a crowd. Le Bon argues that crowds develop a **collective mind**, driven by emotion rather than reason. When people join a group, they lose personal responsibility, become more suggestible, and act based on **instinct and contagion** rather than logic or morality.

He emphasizes that leaders can manipulate crowds through **simple ideas, repetition, and strong imagery**, since crowds respond more to **emotion and symbolism** than to rational arguments. Le Bon believed that this psychology was shaping modern society — influencing revolutions, politics, religion, and social movements.

Key Takeaways:

1. Rapid Emotional Shifts
Crowds experience emotions in extremes, what begins as mild sympathy can escalate into adoration, and a small feeling of dislike can erupt into violent hatred almost instantly. The crowd's shared energy amplifies every sentiment.

2. Emotional Contagion
In a crowd, emotions spread like wildfire. Individuals unconsciously imitate and absorb the feelings around them, losing their ability to regulate their own emotional state.

3. Loss of Rational Control
Rational thought and self-awareness are replaced by instinctive reactions. The more people are swept up in collective emotion, the less capable they are of critical thinking or restraint.

4. Polarization of Feelings
Crowds rarely experience nuance, everything becomes absolute. Someone or something is adored as a hero or condemned as an enemy; there is no middle ground.

5. Collective Hallucination
Crowds can begin to believe their own emotions as truth, perceiving events not as they are but as they feel them to be. This is why myths and exaggerations often take hold in mass movements.

6. Moral Transformation
When emotions take over, a crowd's moral compass shifts. Acts that individuals would never commit alone — violence, destruction, blind obedience — become acceptable or even celebrated within the group.

Movie:
The Great Hack (2019)

This documentary delves into the story of Cambridge Analytica, the controversial data analytics firm that used personal information to influence elections and shape public opinion. Told through the eyes of former employees, investigators, and researchers, the film uncovers how data-driven communication became a powerful, and deeply troubling, tool for political manipulation. It raises urgent questions about privacy, democracy, and the ethics of digital influence in the modern world.

"*People don't want to admit that propaganda works, because to admit it means confronting our own susceptibility, horrific lack of privacy, and hopeless dependency on tech platforms ruining our democracies on various attack surfaces* ".

"*If you want to fundamentally change a society, you first have to break it. It's only when you break it you can remold the pieces into your vision of a new society*".

Key Takeaways:

- **The data from our online activity, our digital trace, isn't simply evaporating**; it's being monitored and stored. All the credit card swipes, web searches, locations, and likes are collected in real time and attached to an identity, giving buyers direct access to our emotional pulse.

- If you feel that the advertisements you receive are exactly what you were expecting, it means that the process of selective targeting is working and has successfully predicted your behavior.

- Not many people bother to read the terms and conditions or privacy policies, a situation that needs to change.

- To send personalized messages, companies need access to people's personal data.

- **Data has surpassed oil in value, making it the most valuable commodity on Earth.**

- "The persuadable", those who are not completely decided on a topic, are the easiest to influence.

- Psychographics should be classified as weapons and protected by every individual as strongly as they protect their property.

- There is a growing movement to have data rights recognized and included in the new human rights framework.

- **Even though Cambridge Analytica no longer exists, some of your data is still being used in ways we aren't fully aware.**

Have a look at the two middle circles.
Which one would you say is bigger?
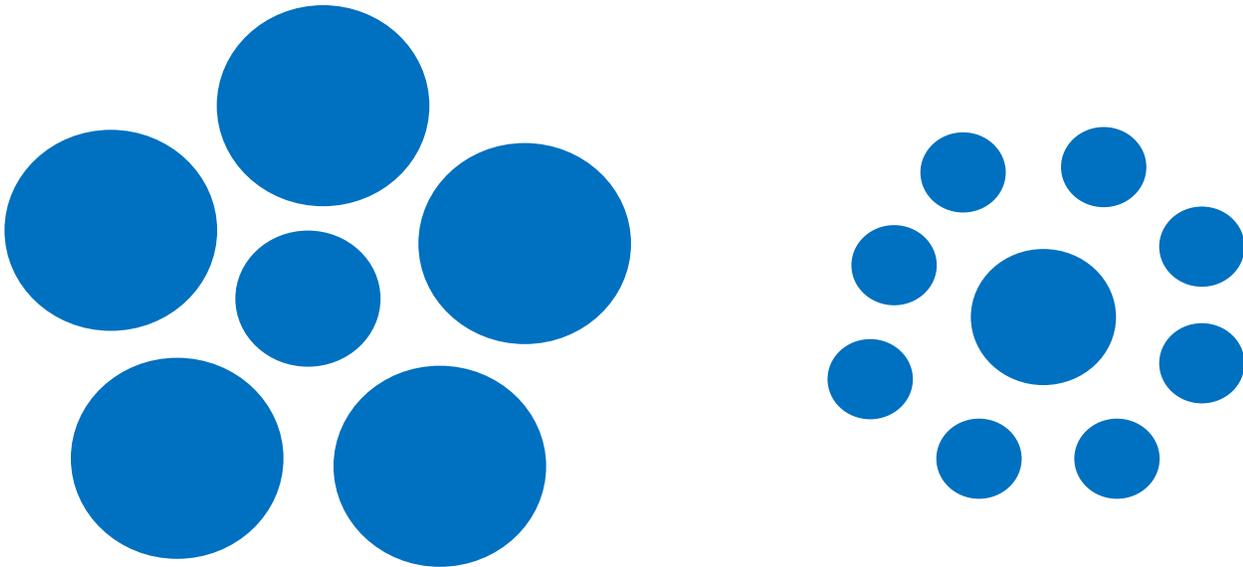
If you chose the one on the right, your answer is similar to that of 99% of the people who were asked this question. The correct answer, however, is that both middle circles are the same size.

Take a moment to measure them.

What makes them appear different are actually the surrounding circles. When the middle circle is placed among larger circles, it seems smaller; when it's surrounded by smaller circles, it seems larger.

You can try this experiment yourself: start by creating two identical circles (you can simply create one and copy-paste it). Leave some space between them so you have room to add the surrounding circles. For one of them, use larger shapes; for the other, smaller ones.

Hint: the same effect occurs when you use other shapes as well.

Thank You for Perceiving...

Meet The Ace Team

The Applied Cognitive Effects function was recently established in HQ SACT to act as a hub of knowledge to drive forward implementation of the NATO Cognitive Warfare concept, and to move the Alliance towards a behaviour-centric approach.

Our team is made up of experts in Behavioural Science, Psychology, Information Operations, PsyOps, Tactical Deception, Wargaming, Red Teaming, and Concept Development.

Let us show how Cognitive Warfare can be used to bring transformation to your approaches.

Thank you for reading this edition of our newsletter. We greatly value your engagement and support as we continue to strengthen this community of interest. We also appreciate the feedback shared on our previous issue and have expanded both the *Strategic Spotlight* and *Cognitive Culture* sections in response. If you have questions, would like to contribute content, or wish to highlight upcoming events, please contact us at hqsact.cognitivewarfare2@nato.int.