Cyber Insight

CyberLegionArmy Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources.
This information is analysis from a strictly cyber perspective.

The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

CyberLegionArmy Group

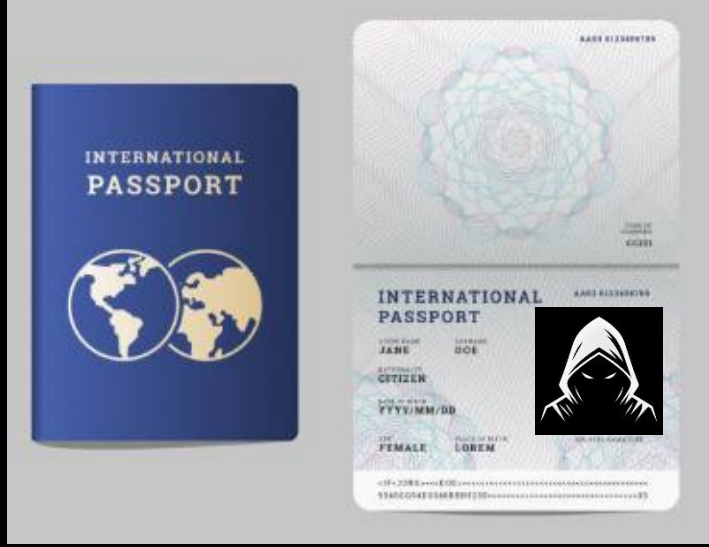
- **Creation date:**
  CyberLegionArmy emerged in October 2025, publicly introducing itself on October 17, 2025, through a manifesto-style video posted on X. Its appearance coincided with an intensification of online publication activities linked to the war in Ukraine, including reports of election interference and disclosures about bot farm infrastructures.

- **Probable Origin**:
  The origin of CyberLegionArmy is deeply rooted in the Russophone diaspora and the radicalization driven by the regime and the Russian-Ukrainian conflict. Its founding members are typically Russophone IT professionals aged between 25 and 45 (developers, administrators, and cybersecurity enthusiasts). They are described as ethical hackers and former employees of the state-linked tech sector (such as ex-Yandex or VK staff) who became hacktivists due to censorship and political alienation.

- **Main strategies:**
  CyberLegionArmy's core approach involves the non-destructive seizure of assets, in which the group successfully compromises propaganda tools—such as bot farms—to hijack accounts and followers. This operational focus is achieved through low-footprint infiltration methods that rely on basic social engineering for credential theft and the use of browser automation tools like Octo Browser to replicate and take control of existing botnet configurations.

- **Geopolitical Motivation:**
  The CyberLegionArmy group is defined by clear ideological and geopolitical motivations, centered on opposing the « Kremlin's authoritarianism » and engaging in information warfare. Their objectives are primarily political, secular, and focused on regime change.

- **Targeted business sectors:**
  CyberLegionArmy focuses exclusively on disrupting Russian state-sponsored disinformation and propaganda networks, targeting bot farms and automated pro-Kremlin accounts to counter Kremlin influence operations. Its operations primarily strike social media platforms and messaging apps like Telegram, VK, and X/Twitter, where regime propaganda is disseminated to shape narratives around the Russian-Ukrainian conflict. By indirectly exposing and hijacking Moscow-funded information warfare tools, the group aims to undermine government-affiliated networks without engaging in broader cyber disruptions.



Identification

CyberLegionArmy is a community of cyber activists advocating for a free Russia—one without dictatorship, censorship, or war. Describing itself as a decentralized "army" of digital fighters, the group went public in October 2025, spurred by a surge in Kremlin disinformation and tightening domestic repression. CyberLegionArmy mainly targets Russian disinformation networks and has gained a politically polarized reputation as a counter-propaganda force. CyberLegionArmy's actions rely heavily on emotional intelligence and cognitive manipulation to recruit supporters and spread its counter-propaganda. The group systematically exploits cognitive biases to shape perception, reduce psychological barriers, and drive participation.

Credits Orange Cyberdefense

Vectors of Influence

1

Narrative Framing

CyberLegionArmy frames its fight as a binary battle between freedom and Kremlin propaganda, using rhetorical slogans that assert a shared objective truth to rally supporters. This gain-frame approach portrays success as an inevitable victory, leveraging optimism bias to motivate prospects by emphasizing positive outcomes over risks.

2

Technical Filter and Initiation

The group places blocks of obscured text, made up of random characters or hexadecimal code, on its website to capture the attention of potential recruits. This digital ritual rewards persistence, fostering a sense of exclusive initiation that boosts loyalty through cognitive investment in the process

3

Illusion of Control and Inclusivity

The "Our Objectives" section on their web site outlines diverse roles, from coding and vulnerability hunting to simply sharing key information, lowering entry barriers for varied participants. This role granularity creates an illusion of control, making each member feel their immediate contribution holds real value and impact.

4

Scarcity and Elite Aspiration

CyberLegionArmy maintains a two-tier structure, separating the open group from the elite "core" (kostyak), accessible only by invitation and vote for the most reliable members. This scarcity mechanism drives deeper engagement by appealing to aspirations of elite status and exclusivity among recruits.

5

Social Proof and Success Legitimacy

CyberLegionArmy builds credibility by claiming tangible wins, such as seizing 300 pro-Kremlin accounts and causing over a million dollars in estimated influence loss. This social proof positions the group as effective and bold, enhancing collective agency and trust among sympathizers.

Cyberdefense

Credits Orange Cyberdefense

Emotional Intelligence

1

Cognitive Curiosity: Obscured text blocks on their web site create an information gap that turns the page into a puzzle and activates the dopaminergic reward loop associated with curiosity. This engagement test filters for technically capable users and rewards them with a sense of exclusive initiation, increasing perseverance and loyalty.

2

Self-Efficacy: By listing very diverse contribution options (“someone writes code, someone spreads information”), the group lowers the entry threshold for all profiles. This granularity strengthens perceived self-efficacy among novices and leverages the illusion of control, as everyone feels able to make a meaningful contribution.

3

Reciprocity and Anonymity Assurance: The promise to “guarantee anonymity and careful handling” of submitted data creates a moral debt for informants and reduces risk aversion. This assurance applies the reciprocity principle, making it more likely that individuals will share sensitive information.

4

Elite Aspiration and Scarcity Bias: The two-tier structure (Open Group vs. closed “kostyak” core) exploits scarcity bias to stimulate deeper engagement. Invitation- and vote-based access to the core strengthens members’ social identity and pushes them to contribute more in order to reach elite status.

5

Social Proof (Social EI) and Action Legitimization: The group uses social proof by normalizing leaks as a collective standard of action within the movement, reducing fear of illegality. Claims of concrete impact, such as causing an estimated one-million-dollar loss, reinforce perceived effectiveness and attract new recruits

6

Emotional Contagion and Militant Imagery: Military-style imagery (“army”, “hero”) and rhetorical slogans are designed to trigger emotional contagion, generating urgency and shared outrage against censorship. This language emotionally anchors the reader in a militant mindset, transforming passive dissatisfaction into a call for immediate action.

orange Cyberdefense

Credits Orange Cyberdefense

CyberLegionArmy Website Deconstruction

1. The Rhetorical Slogan and Header (Framing Effect)

The site immediately presents its core slogan: **"Свободу не заблокировать — правду не удалить"** (Freedom cannot be blocked — truth cannot be deleted).

It identifies the group as a "community of cyber-partisans fighting for a free Russia". It uses the **framing effect** by immediately portraying the struggle as an "inevitable victory" (a gain frame) against a fragile "wall of propaganda

2. Obfuscated Text Blocks (Information Gap Theory)

In the web site, the group includes lines of random/hexadecimal characters.

The Cyber Intelligence Bureau identified several notable blocks containing intriguing strings: Block 0x4B5D: "KIVING…", Block 0x5FAD: "DIE…", Block 0x8AD0: "TING…", Block 0x731A: "NGC…", Block 0x8163: "INBEI…", Block 0x2F4D: "SPARING…", Block 0x5BDC: "NIGHING…", and Block 0x6AB7: "VERSING…".

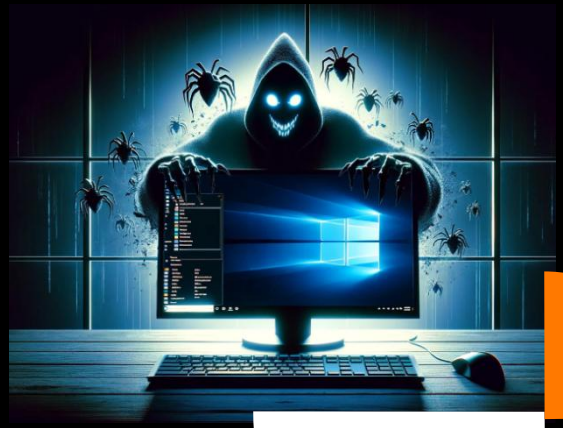
We could potentially interpret them such as: « KILLING, DYING, ACTING, ENGINEERING, BEING, SPARING, OPERATING AT NIGHT, EXPRESSING »

Moreover, root access and a password for the IP address “95[]173[]136[]70” associated with “kremlin[]ru” are explicitly displayed, as if the group had obtained access. This creates a sense of satisfaction and excitement for technology enthusiasts and the hacking community.

The Open Group as a Portal (Gamification and Cohesion)

The "Открытая группа" "(Open Group)" is positioned as the initial entry point for all individuals who have made a "useful contribution," and is described as the "коллективный разум" (collective intelligence) of the movement

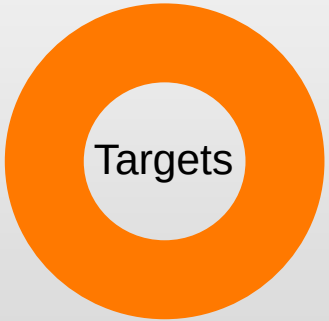
Tools and Techniques used by CyberLegionArmy



Technique	Description
Octo Browser	A specialized anti-detection browser used with automated profiles to manage multiple sessions. It is utilized to emulate and hijack botnet configurations, allowing the group to seize control of existing account sessions.
Social Engineering Tools	These include manual techniques or basic tools, such as phishing kits or credential stuffers. They are employed for credential theft to gain unauthorized access to bot farms without relying on complex zero-day exploits.
Custom Mirroring Scripts	Proprietary, home-made code, often inferred to be Python or JavaScript based. These scripts duplicate and override existing account configurations to automate the dissemination of anti-regime counter-propaganda.
OSINT Tools for SIM Tracing	Open Source Intelligence software, such as custom scrapers or geolocation APIs. These tools are used to trace the geographic provenance of SIM cards utilized by botnets across various countries, exposing the global reach of disinformation networks.
Proxy Chaining and VPNs	Anonymity tools, including Tor or rotating proxies. They are essential for protecting the group's identity during infiltration, especially when conducting operations across multiple jurisdictions to evade tracking by surveillance agencies.

Credits Orange Cyberdefense

Targets



100% of their targets are state propaganda machines

Note

The group CyberLegionArmy exclusively targets the media and “disinformation” sectors, representing all known hostile activities to date. Their confirmed operation, the "BotFarm Takeover" of October 2025, specifically targeted a pro-Kremlin bot farm, a state-affiliated disinformation apparatus. This approach aims to undermine state propaganda and erode the regime's narrative control by turning enemy tools against propaganda. This tactic could also be used in NATO countries for electoral manipulation or major geopolitical actions.

Most Probable Hypothesis on CyberLegionArmy's Future Activities

Future Targets
The most plausible adversarial strategy for CyberLegionArmy involves iterative disruptions of bot farms and sustained psyops. The group will likely expand its focus from the initial successful operation to include the progressive hijacking of more pro-regime Telegram channels. This sustained approach will maintain their primary target focus on the Media and Disinformation sector, while the potential for leaks exposing state operations implies future targeting of Government-Affiliated Networks.

Hybrid Methods
The group is expected to scale its operations by enhancing OSINT techniques, such as advanced SIM tracing, combined with browser hijacking variants coordinated via Telegram. Its tactical evolution is likely to involve enhanced recruitment and alliances (e.g., with Anonymous) to support multi-operation campaigns. Furthermore, the group may integrate more sophisticated methods, potentially leveraging generative AI for automation, such as creating deepfakes to amplify its counter-propaganda.

Systemic Impacts
The main foreseeable impact of these activities is the incremental erosion of Kremlin influence, potentially resulting in cumulative damages exceeding $5 million. By persistently transforming propaganda channels into platforms for "truth" and dissent, CyberLegionArmy will continue to boost dissident morale and normalize the act of leaking sensitive information. However, increased success will inevitably lead to heightened crackdowns by the FSB and potentially strain platform moderation globally due to the rise of copycat operations.

Credits Orange Cyberdefense

The most dangerous hypothesis

The Most Dangerous Scenario
The most dangerous future disruptive scenario is a coordinated "Digital Uprising" cascade. This scenario involves CyberLegionArmy succeeding in infiltrating and seizing control of financial botnets and election interference tools. Such a massive operation would have the potential to trigger global market panic and cause voter manipulation reversals.

Targets and Sectors Targeted
The group could transition from its current focus to direct strikes against Government-Affiliated Networks. While CyberLegionArmy's current known activity is high against the Media and Disinformation sector (targeting Russian entities), the most dangerous hypothetical scenario assumes a significant escalation in target type:

- Financial Institutions: Specifically, the scenario predicts financial botnets as targets.
- Election Systems: The group targets election interference tools.
- State Media: These entities would remain a target.

Methodologies
To carry out this scenario, CyberLegionArmy would need to evolve substantially beyond its current "low-footprint" tactics such as using Octo Browser and social engineering for credential theft. This evolution might include leveraging large volumes of compromised social media accounts, expanding credential theft through insider collaborators, and deploying advanced generative AI technologies to produce deepfakes for psychological operations.

Potential Consequences
Socially and politically, such attacks would erode trust in institutions, likely triggering protests and unrest. Most critically, these events could escalate hybrid conflicts, intensifying tensions between NATO and Russia.

Credits Orange Cyberdefense

Bilateral Risks & Missing Perspective

While no direct statements from Russian authorities, such as the FSB, have been identified regarding CyberLegionArmy as of December 2025, similar anti-regime hacktivist groups have been labeled by Russian sources as "foreign-sponsored threats" or "hybrid sabotage."

Bilateral risks include potential escalation in cyber-retaliations, where non-destructive operations like bot farm hijacking could provoke symmetric responses from state actors, impacting NATO allies through increased disinformation or infrastructure targeting, as noted in recent analyses of hybrid conflicts.

This underscores the need for balanced monitoring to assess broader geopolitical implications.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense