THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

October 24, 2024

Russian Strategic Information Attack for Catastrophic Effect

Russia's SIA provides the Kremlin with a non-kinetic means to inflict overwhelming damage to its adversaries during strategic conflict, very likely reserved for "large-scale war".

Russian SIA has two primary components: (1) "psychological attack" and (2) "technical attack", each with different but overlapping desired effects.

Russian SIA is part of the Kremlin's strategy for conflict escalation management, enabling Moscow to "escalate" with non-kinetic strategic capabilities to force "de-escalation" via peace negotiations.

Executive Summary

Russian strategic information attack (SIA) conceptualizes the Kremlin's capability to inflict strategic damage to its adversary's national critical infrastructure (NCI) via non-kinetic means.[1] According to Russian strategy and doctrine, SIA is very likely reserved for a conflict defined as "large-scale war" in Russia's official military doctrine — akin to the employment of Russia's strategic nuclear forces. As of this writing, Russia has almost certainly not conducted an SIA against its adversaries. However, the targets for SIAs almost certainly align with Russian information attacks against critical infrastructure in the West over the past decade, especially NCI.

As defined in Russia's "information confrontation" strategy, Moscow conceptualizes two distinct types of non-kinetic SIAs: "psychological attack" (strategic influence operations) and "technical attack" (strategic cyberattack). Russia's SIA is part of the Kremlin's "conflict escalation management" strategy, providing Moscow with a non-kinetic escalatory measure designed to seize the advantage in a conflict, force its adversary to negotiate, and de-escalate the conflict. In the event Russia decides to conduct an SIA against Western NCI — as framed by the Cybersecurity and Infrastructure Security Agency (CISA) — the event would serve as an indicator that the Kremlin believes it is engaged in strategic conflict. Thus, in such a scenario, CISA's sixteen NCI categories are at risk of strategic cyberattacks intended to cause lasting, widespread damage. The former — which Kremlin-linked think tanks theorize can include the "malicious use of artificial intelligence (MUAI)" — is used to induce the rapid and catastrophic deterioration of the internal political situation in the target country. The latter is intended to cause strategic damage to the technical aspects of NCI, such as networks and systems.

Western public and private industry leaders and Russia-focused defense analysts should account for Russia's potential to conduct SIAs, especially in training events and exercises. Additionally, public and private sector clients should use the Recorded Future® Intelligence Cloud to identify Russian state-sponsored cyberattack tactics, techniques, procedures, and indicators and implement associated mitigations. Although there is significant emphasis placed on Russian cyber capabilities that can target NCI, it is equally important to account for Russian strategic "psychological attack" and its incorporation of artificial intelligence. Moreover, Western industry leaders and experts should anchor Russia's strategic actions in Moscow's official strategy, doctrine, and policy to determine the Kremlin's intentions rather than assuming Russia's actions are conducted simply to inflict catastrophic damage with no desired strategic end state.

[1] Insikt Group will use the acronym SIA for strategic information attack throughout this report, acknowledging it is not a commonly accepted acronym in Russian and Western parlance.

Key Findings

- Russia's SIA provides the Kremlin with a non-kinetic means to inflict overwhelming damage to its adversaries during strategic conflict; it is very likely reserved for "large-scale war", but the targets can be similar to those attacked during lower-intensity conflicts.
- Russian SIA has two primary components: (1) "psychological attack" (strategic information operations) and (2) "technical attack" (strategic cyberattacks), each with different but overlapping desired effects.
- An NCI that supports both private and public sector assets, such as communications infrastructure that supports commercial and government organizations, is very likely the most attractive target for a Russian SIA.
- Russian SIA is part of the Kremlin's strategy for conflict escalation management, enabling Moscow to "escalate" to force "de-escalation" via peace negotiations — akin to Russian military theory on the use of nuclear weapons.
- Western cybersecurity defense efforts should endeavor to account for the "psychological attack" aspect of Russian SIA as efforts continue to establish mitigations for potential Russian "technical attacks".

Doctrinal Anchoring

As of this writing, Russia does not have a publicly available policy or a singular strategy and doctrine document that specifically addresses the use of SIAs. To determine Russia's approach to information attacks during strategic conflicts, Russia's official policy and strategic documents that frame the Kremlin's thought process concerning efforts to target NCI and the potential implications of a strategic "psychological attack" against Russia's adversaries are referenced throughout this report. Although there are similarities in the employment of information attacks during lower-intensity conflicts, this research applies to Russia's use of information attacks during "large-scale war" as defined in Russia's official military doctrine.[2] [3] Accordingly, the analysis herein excludes lower-impact, state-sponsored information attacks outside of a "large-scale war" as well as cyberattacks from Russian financially motivated and cybercriminal threat actors. According to Russian national policy, cyber is unique in that it's both a warfighting domain and a strategic capability that enables activities to target an adversary's "psychological security" and "information processing systems".[4] [5]

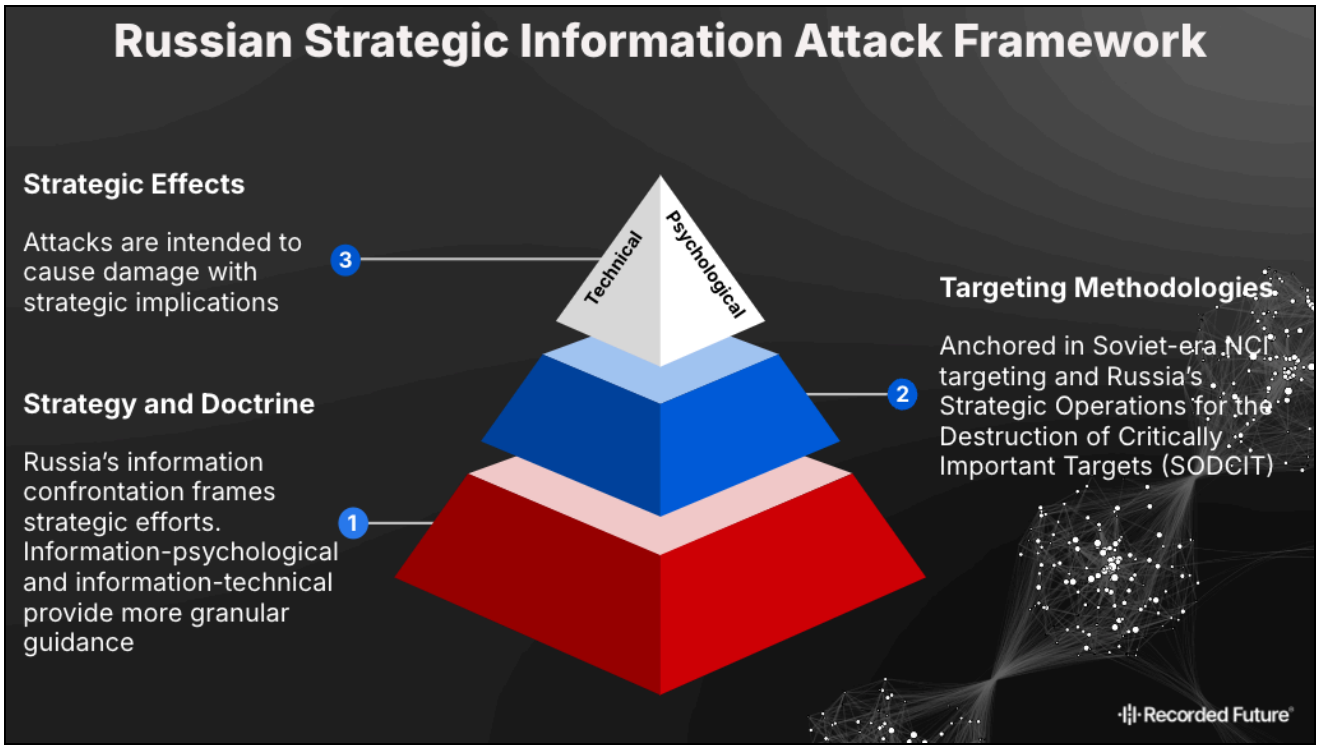

Figure 1: *A conceptualization of Russia's SIA framework that highlights links between strategy and doctrine, legacy and modern targeting methodologies, and desired strategic effects (Source: Insikt Group)*

[2] Russia's official military doctrine defines four specific categories of conflict. From lowest to highest intensity, the categories are as follows: (1) armed conflict, (2) local war, (3) regional war, and (4) large-scale war (almost certainly synonymous with world war). The latter, according to Russia, involves employing all of Russia's capabilities, including strategic weapons, to achieve victory against its adversary.
[3] *https://thailand.mid[.]ru/en/o_rossii/vneshnyaya_politika/voennaya_doktrina_rf/*
[4] "Psychological security" frames Russia's view on the cognitive stability and unity of a country. Countries with degraded psychological security are more susceptible to destabilizing influence operations. Conversely, countries with strong psychological security are more resilient to influence operations.
[5] *http://www.scrf.gov[.]ru/security/information/DIB_engl/#:~:text=The%20Doctrine%20defines%20the%20information,networks%2C%20information%20technologies%2C%20entities%20involved*

Information Attacks For Strategic Conflict

Russia's conceptualization of SIA is linked to military theories that frame other forms of strategic attack, such as the employment of Russia's nuclear triad and the use of conventional military means to achieve strategic effects. The distinction, however, is that Moscow will be able to achieve the desired strategic effects without the physical destruction that accompanies using nuclear weapons. Within Russian strategy, specifically "information confrontation", the Kremlin highlights two distinct lines of effort and targets for strategic actions in the "information sphere", which includes the cyber domain: (1) adversary psychology and (2) adversary information processing systems.[6] The former involves activities that would be framed as "influence operations" in Western defense parlance, whereas the latter involves efforts to undermine, disrupt, degrade, or destroy adversary national critical information systems and other NCI.

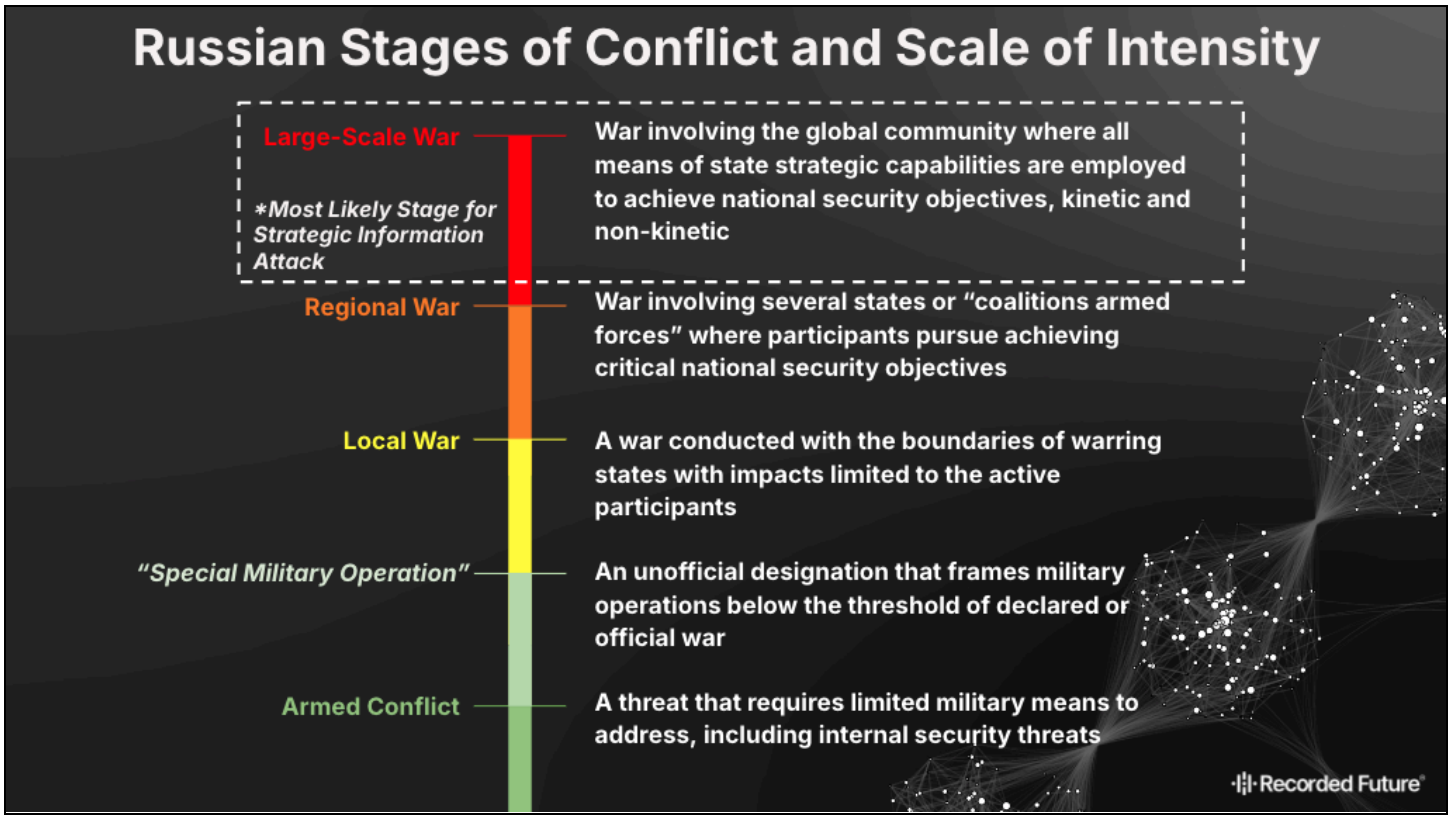

Figure 2: *Russia's stages of conflict and war and their associated levels of intensity. "Special Military Operation" is not an official category of war in Russia's military doctrine and was created to account for Western-style military operations below the threshold of declared war; it is used by Russia to describe its conflict against Ukraine (Source: The Military Doctrine of the Russian Federation and Insikt Group)*

[6] Russia's official policy, titled "Doctrine of Information Security of the Russian Federation", frames the "information space" or "information sphere" as the cognitive and digital domain. Specifically, Russia defines the domain as "a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet (hereinafter referred to as the "Internet"), communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations".

Although there is widespread public awareness of Russian cyber capabilities, Russian state-sponsored cyber threat actors have almost certainly not conducted cyberattacks that resulted in strategic effects, such as long-term disruptions of portions of power grids. Similarly, Russia has yet to conduct influence operations that have resulted in the "rapid degradation" of a target country. Thus, while this research acknowledges instances of Russian information attacks to disrupt or degrade NCI functionality, such as information attacks against Ukrainian infrastructure, information attacks that have resulted in the destruction or complete inoperability of NCI have not been observed. These attacks, based on Russia's approach to "large-scale war", will very likely be reserved for strategic conflict where other strategic capabilities are employed, such as nuclear weapons. Additionally, Russia's strategy for conflict escalation management, called "escalate to de-escalate" in Western defense parlance, provides further insights into the Kremlin's conceptualization of the phases or stages of conflict where strategic capabilities are employed.[7]

Strategic Influence Operations — Psychological Attack

Russia's strategy for information confrontation frames efforts that are designed to shape the information space in Moscow's favor. Specifically, one of the subset lines of effort with the information confrontation strategy, "information-psychological", calls for activities designed to destabilize an adversary country's internal political situation. In extremis, these actions can be conducted to induce "regime change". Substantively, the modern adaptation of Russia's influence operations is similar to Soviet-era "active measures", which exploited existing internal societal, political, racial, and religious fissures to degrade national cohesion and stability. However, Russian strategic psychological attack should not be confused with normal efforts to manipulate the information space, such as Russia's long-espoused claim that the United States (US) is engaged in aggressive foreign policy designed to destabilize the Russian Federation via regime change.[8] [9]

According to Kremlin-linked think tank analysis, specifically from the Russian International Affairs Council (RIAC), Russian military theorists are considering how emerging technologies can support strategic influence operations. Specifically, 2024 RIAC analysis frames a capability called "malicious use of artificial intelligence (MUAI)", and its potential ability to induce "rapid deterioration" of the internal political situation within a target country. MUAI involves using mass-produced, high-quality AI content that supports Russia's efforts to target the "psychological security" of the target country.[10] More specifically, RIAC assesses that AI-produced deepfakes that are difficult for someone to determine whether they are real, such as a deepfake of a national leader giving a national address, have the ability to induce widespread chaos in a target country.[11] Russia very likely envisions former KGB analyst Igor

[7] Over the past decade, Western defense analysts have assessed a Russian concept called the "Gerasimov Doctrine", which is linked to an older concept called the "Primakov Doctrine". Despite divergent views on the date and origin of the concept, each of the doctrinal approaches identify phases of conflict and the use of state means to achieve Moscow's national security objectives.
[8] *https://www.rt[.]com/russia/552943-biden-russia-regime-change/*
[9] *https://www.rt[.]com/news/564123-bolton-regime-change-putin/*
[10] "Psychological security" is framed as the societal cognitive stability within the target nation. For example, a nation Russia determines as being politically polarized or experiencing domestic unrest that is destabilizing the functionality of the country, would be vulnerable to psychological security threats.
[11] *https://russiancouncil[.]ru/en/analytics-and-comments/analytics/malicious-use-of-ai-and-challenges-to-psychological-security-future-risks/?sphrase_id=143813599*

Panarin's assessment that internal societal polarization could lead to the "balkanization" of the US or a second Civil War.[12]

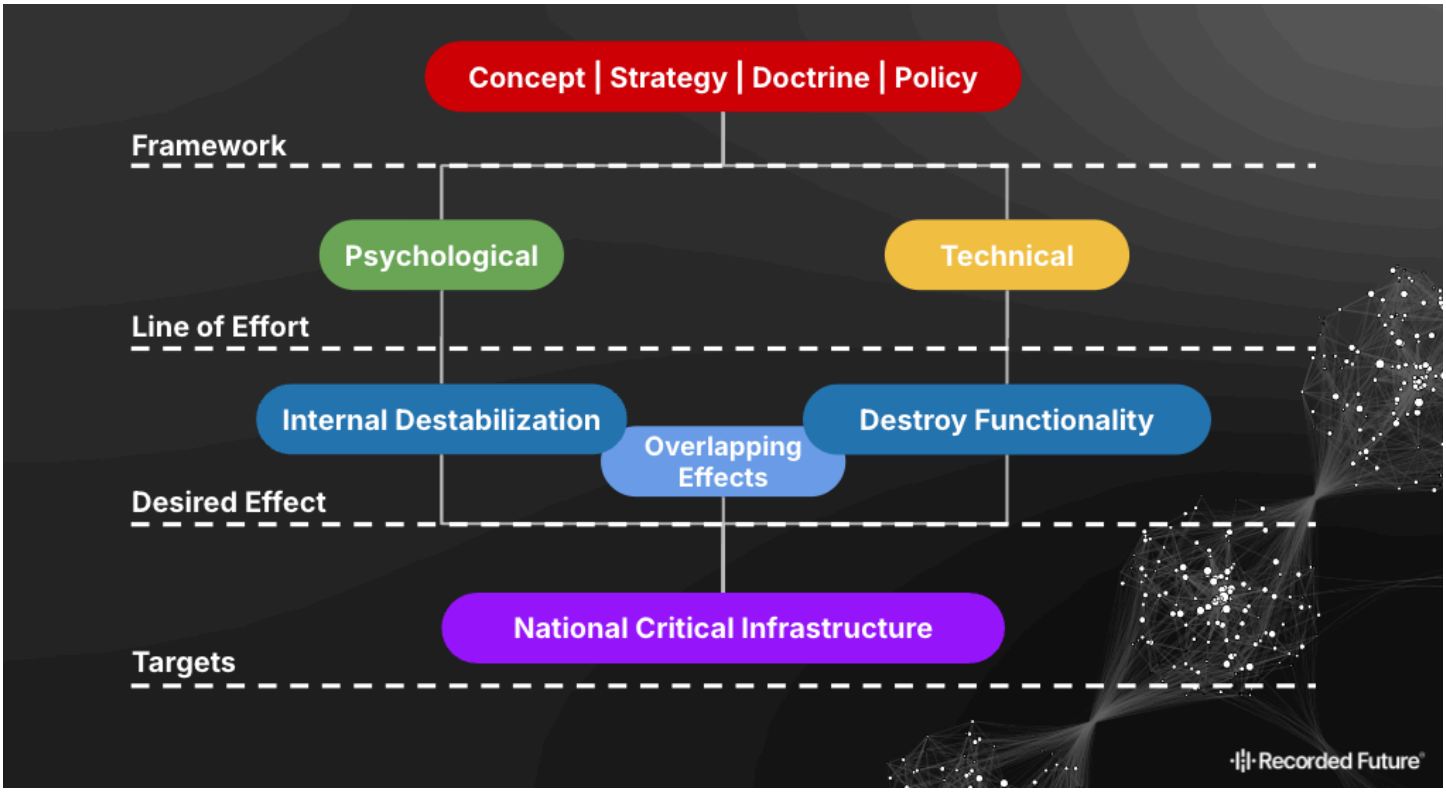

Figure 3: *Assessed Russian approach to SIA (Source: Insikt Group)*

Strategic Cyberattack — Technical Attack

Russia's information confrontation strategy also calls for attacks against an adversary's "information processing systems", actions which the Kremlin designates specifically for "wartime". These attacks are designed to target systems that "receive, collect, process, and transmit information". Although Russia's information-technical strategy does not provide specific targets, they almost certainly include public- and private sector-managed NCI. Russia's cyberattacks against targets during "large-scale war" in alignment with its information-technical strategy are likely similar to cyberattacks conducted during times of heightened geopolitical tensions or lower-intensity conflicts (for example, Ukraine).[13] What would very likely differentiate strategic information-technical cyberattacks is the intent to cause strategic damage to the adversary's NCI versus temporary disruptions in functionality.

Russia's cyber activities during its continued war against Ukraine very likely highlight distinctions in Russian escalation of force, including non-kinetic options, during military operations. Although Western countries characterize Russia's invasion of Ukraine as "full-scale", Russia's official military doctrine

[12] *https://www.rt[.]com/russia/panarin-usa-collapse-economy-905/*
[13] According to Russia's official military doctrine, Moscow does not categorize its military operations in Ukraine as a war but a "Special Military Operation". This operational designation likely nests between "armed conflict" and "local war" within Russia's military doctrine.

does not. In Russian defense parlance, "full-scale" war would be synonymous with "large-scale war", which Moscow considers akin to global war.[14] Although Russia has conducted cyberattacks targeting NCI, attacks that have resulted in strategic effects, such as the destruction of Ukraine's national communications or power grid, have not been observed.

Military Strategies Highlight Strategic Targets

As previously stated, Russia's publicly available strategy documents do not provide specific targets for information attacks during strategic conflict. Because of this, our research references Soviet-era strategies and modern Russian strategic conflict concepts. Based on our understanding of Russian targeting efforts, targets noted in legacy and modern military doctrine provide insights into the targets Russia would prioritize. As part of operational planning, Russia very likely determines which targets are better suited for attacks with "psychological" or "technical" effects.

Soviet-era Target Designation

During the Soviet era, defector Viktor Suvorov revealed that Russia's Main Intelligence Directorate of the General Staff (GRU) conducted NCI targeting during strategic conflict using an anthropomorphic model. The targets, according to Suvorov, included individuals and assets the Soviet Union determined were critical to the adversary country's functionality and ability to execute war. Notably, Suvorov's disclosure of GRU targeting methodology in the 1980s does not address the use of cyber capabilities.

Suvorov's targeting model is divided into four categories: (1) the "Brain and Reserve Brain", (2) the "Nervous system", (3) the "Heart and Blood Supply", and (4) the "Teeth". Each of these categories corresponds with Russia's framing of NCI and nationally critical individuals. Although these targets are designated for GRU covert action in Suvorov's model, they are also almost certainly suitable targets for Russian "psychological" or "technical" targeting.

Suvorov's Targeting Framework	
Anthropomorphic Classification	**National Critical Target Equivalent**
Brain and Reserve Brain	National and local leadership
Nervous system	National communications
Heart and Blood Supply	National energy infrastructure
Teeth	Nuclear weapon capabilities

Table 1: *The Soviet era, GRU targeting framework for covert operations during a time of war (Source: Viktor Suvorov's The Inside Story of Soviet Special Forces and Insikt Group)*

[14] *https://thailand.mid[.]ru/en/o_rossii/vneshnyaya_politika/voennaya_doktrina_rf/*

Modern Strategic Targeting

To frame Russia's modern approach to strategic information targeting, we cite two Russian sources: (1) the Doctrine of Information Security of the Russian Federation, and (2) the Defense Ministry's Strategic Operations for the Destruction of Critically Important Targets (SODCIT) framework. The former source highlights Russia's conceptualization of the information space, which includes cyber, and inherent strategic threats.[15] The latter source provides insights into how the Kremlin views targets that fall within NCI.

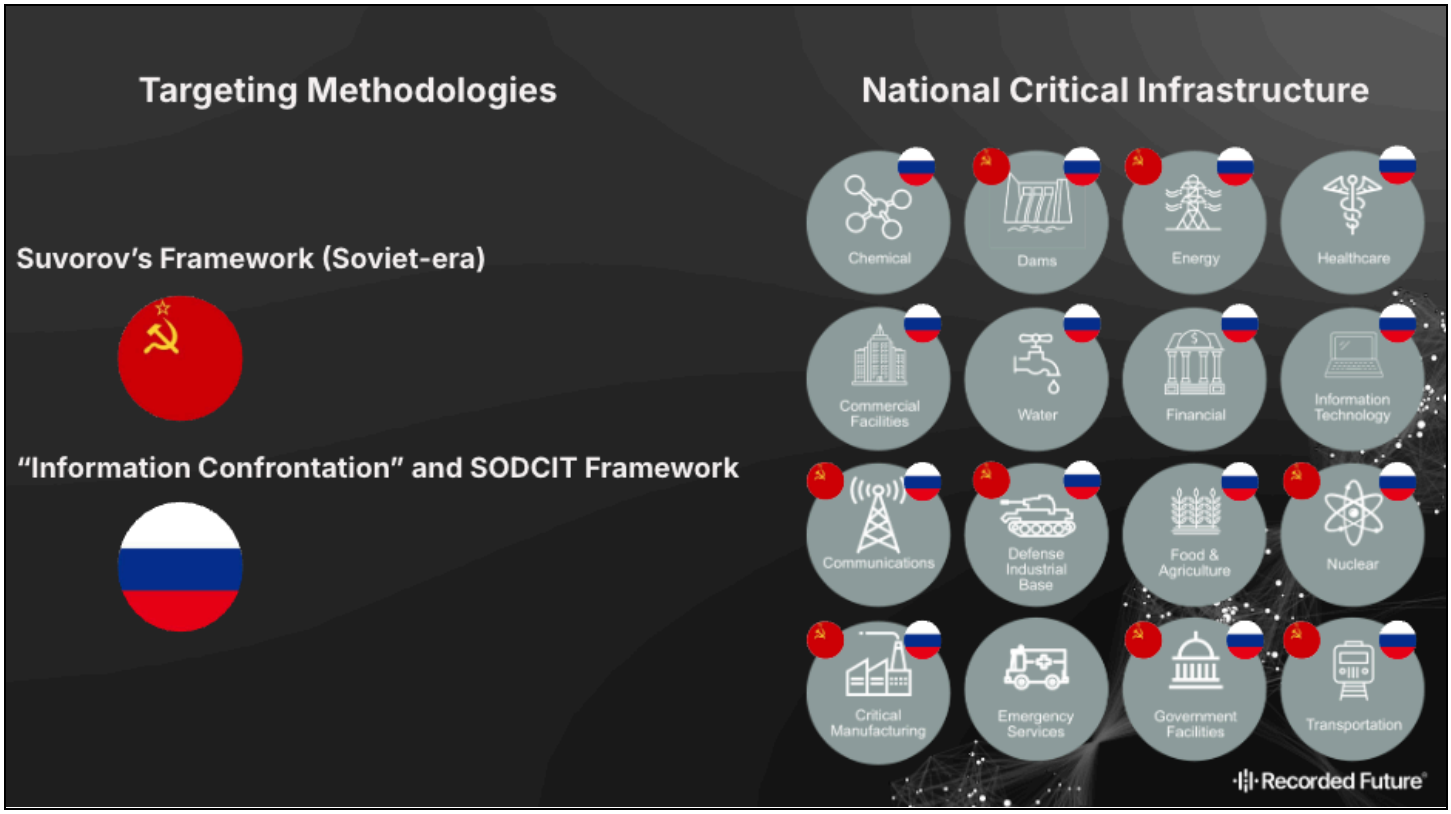

Figure 4: Russia's *Soviet-era and modern targeting frameworks against NCI as defined by CISA (Source: Insikt Group)*

Russia uses the doctrinal term "information sphere" to capture threats and opportunities. As part of Russia's worldview and threat perception, the Kremlin believes that Russia's adversaries conduct operations in the information sphere, including cyber activities, to threaten Russia's internal stability. Framed as "influence operations" in Western parlance, Russia's information security policy highlights the "psychological" effects of adversary country activities that are designed to "destabilize the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other States. Religious, ethnic, human rights organizations and other organizations, as well as separate groups of people, are involved in these activities and information

[15] *http://www.scrf.gov[.]ru/security/information/DIB_engl/#:~:text=The%20Doctrine%20defines%20the%20information,networks%2C%20information%20technologies%2C%20entities%20involved*

technologies are extensively used towards this end".[16] Additionally, Russia's information security policy frames the defense of Russia in the information sphere as a national security objective that is critical to the stability of the Russian Federation.[17]

The Russian Defense Ministry's SODCIT concept highlights the Kremlin's kinetic targeting approach. According to the Center of Naval Analysis, SODCIT is "an operation designed to inflict a combination of material and psychological damage, while limiting civilian casualties and avoiding unintended escalation. The operation is aimed at critically important objects, or targets, of the military, economic, and political-administrative types." Additionally, the concept prescribes targeting "the systems of command of state, armed forces, and force groupings: intelligence, surveillance, and reconnaissance (ISR) and communications centers, key objects of economic infrastructure and quality of life, objects of communal infrastructure, and objects of mass public information." These targets, according to Russia's conceptualization, include terrestrial and space-based NCI.

Desired Strategic Effects

According to Soviet-era defector disclosures, specifically Viktor Suvorov, and Russia's modern military strategy and doctrine, Russian strategic attacks are intended to undermine a target country's capacity and willingness to engage in prolonged conflict while not inducing an escalation. Additionally, the attacks are nested within Russia's conflict management concept, "escalate to de-escalate", where Russia conducts an escalatory military measure designed to compel its adversary to accept negotiations on Moscow's terms. As noted in Russia's SODCIT doctrine, targets are selected in a manner that reduces the risk of "significant" civilian casualties, doesn't "lead to an ecological disaster, and does not provoke further escalation". Historically, Russian military theorists have pointed to the US use of nuclear weapons against Japan — an escalatory attack designed to induce peace negotiations — as an exemplar of the de-escalation of tension strategy. Thus, Russia could employ strategic cyber capabilities to achieve the same result.

Russia's legacy and modern strategies suggest that adversary NCI can be subjected to psychological attacks, technical attacks, or both, depending on the target. For example, adversary communications can be targeted to support Russia's efforts to shape perception or induce significant internal instability, including via MUAI. Similarly, adversary communications can be a target for technical attacks to degrade the ability of national leadership to disseminate information, such as Emergency Alert Systems. However, some targets are better suited for psychological attacks than technical attacks and vice versa. Russia could decide to engage in psychological attacks designed to undermine faith and confidence in an adversary's food and agriculture industry, such as disseminating narratives that food is contaminated and unsafe for consumption. Separately, adversary information technology is a better target for Russian technical attacks, designed to degrade or destroy the ability of the target country to ingest, transmit, and analyze information (see **Figure 5**).

[16] *http://www.scrf.gov[.]ru/security/information/DIB_engl/*
[17] *http://www.scrf.gov[.]ru/security/information/DIB_engl/#:~:text=The%20Doctrine%20defines%20the%20information,networks%2C%20information%20technologies%2C%20entities%20involved*

Psychological Effects

The primary target of Russian strategic psychological attacks is the collective perception of the citizenry in the target country, which includes government and military personnel. Although the specific desired effects can vary, the overarching goal is to induce internal instability within the target country and erode confidence in NCI, which includes national leadership and government institutions. These actions likely include unrest that requires national leadership to evoke emergency powers to restore the rule of law and government authority. While engaged in "large-scale war", Russian psychological attacks could attempt to convince the target country's populace that NCI is either inoperable, degraded, or destroyed, claims that could be false or true. In a psychological attack, Russia will likely conduct influence operations via social media, compromised television or radio communications, or fabricated national messages posing as the adversary country's national leadership. For example, Russian information efforts could suggest that financial institutions are experiencing significant disruptions or that energy infrastructure is at risk of catastrophic failure. As noted in Russia's SODCIT doctrine, the intent is to drive the target country's national leadership to seek out and accept a diplomatic off-ramp to the conflict, driven by an uprising of the domestic populace desirous of a return to pre-war normalcy.

Figure 5: *Hypothetical Russian SIA against adversary NCI. As part of this hypothetical, this graphic highlights how Russia could decide to conduct psychological or technical attacks, or both, against NCI, according to Russian strategy and doctrine. NCI categorization derived from CISA. (Source: Insikt Group)*

Technical Effects

As previously mentioned, the primary target of Russian strategic technical attacks is the target country's information processing systems, which include civilian, government, and military assets. The desired effects are long-lasting and widespread system interruptions or destruction designed to degrade the functionality of the adversary's NCI. By extension, Russian strategic technical attacks are intended to undermine the adversary's ability to manage domestic national processes and execute strategic conflict. In such an attack, Russia could decide to target its adversary's power infrastructure to cause long-lasting energy blackouts or significant disruptions to national secure networks to undermine the ability to transmit national critical information. According to Russia's conflict escalation management strategy, these actions are intended to de-escalate tensions by suggesting that the Kremlin can conduct increasingly destructive attacks should the war persist.

Overlapping Effects

The sole Russian doctrinal concept that addresses the potential for overlapping effects is SODCIT, which primarily addresses the use of kinetic capabilities. A Russian technical attack against an adversary's national communications infrastructure can also have the effects of a psychological attack against the target country's citizenry. Conversely, a psychological attack designed to convince the adversary country's citizenry to believe the financial infrastructure is disrupted could induce people to attempt to withdraw funds en masse (known as a run on the bank) and cause technical disruptions. Despite our ability to hypothesize this type of attack, it's notable that there is no reference in publicly available Russian strategy documents addressing attacks specifically intended to cause the strategic effects of both a technical and psychological attack.

Outlook

As Russia-West geopolitical tensions continue to escalate, the potential for Russia to employ SIAs against Western NCI increases, especially during a "large-scale war". Although Russia has long engaged in cyber activities against the West, strategic cyberattacks will very likely be distinct in that they cause lasting and widespread effects. Because of this, Western private- and public-sector leaders responsible for managing NCI should not mistake a financially motivated Russian ransomware attack, for example, with a Russian state-sponsored strategic cyberattack targeting the same infrastructure.

Governments and corporations involved with NCI should continue enhancing cybersecurity defense capabilities while also considering contingencies if defenses fail. Moreover, industry leaders should cooperate to develop redundancies that can limit the effects of Russian SIA on NCI, especially where public and private infrastructure overlap, such as communications infrastructure. Whether industry leaders engage in private red team cybersecurity exercises or participate in international events, such as Cyber Polygon, scenarios that emulate Russian strategic cyberattacks will likely help identify innovative solutions to mitigate the effects of Russian efforts.

As industry leaders consider efforts to account for and counter Russian strategic cyberattacks, establishing mitigations for Russian "psychological attack" is a significant challenge, especially as Russia continues to develop new strategies in existing influence operations. Concerning Russia's strategy for MUAI, industry leaders and specialists should focus on developing artificial intelligence detection capabilities that support efforts to monitor, detect, and disseminate findings concerning Russia's strategic activities in the "information sphere".

Western, Russia-focused defense experts and analysts should not discount Russian official strategy, doctrine, and policy when assessing the Kremlin's intentions, especially in the open-source domain, where access to sensitive information is lacking. In the event Russia-West tensions escalate to a strategic conflict, anchoring Moscow's actions in Russia's doctrine will likely support efforts to provide predictive analysis concerning Russia's next actions and strategic intentions. Specifically, in the event Russia conducts an SIA against the West, the Kremlin's desire to inflict catastrophic damage to the West is fueled by the intent to compel the West to capitulate to Moscow's terms during potential peace negotiations.

Appendix A: Hypothetical Russian Strategic Information Attack Scenario

Since there is no real-world case study of Russian SIA, as framed by Russian strategy and doctrine, to analyze, the following serves as a scenario in which Moscow employs its strategic cyber capabilities as described above.

Scenario: *The Kremlin has determined that tensions with the North Atlantic Treaty Organization (NATO) have escalated to "large-scale war", per Russia's military doctrine. During discussions with the General Staff of the Russian Federation, Russian president Vladimir Putin decided to authorize the use of strategic capabilities but not the employment of nuclear weapons, high-yield conventional weapons, or covert sabotage. These actions are intended to escalate the conflict against NATO and force the alliance to negotiate an end to the conflict on Moscow's terms. Putin orders the Russian intelligence services to conduct concurrent strategic attacks in line with Russia's "information confrontation" strategy, both "information-psychological" and "information-technical" to induce catastrophic damage to NATO countries. The following hypothetical attacks occur concurrently:*

Strategic Psychological Attack: Russia's intelligence services, in concert with Russia's state media apparatus, engage in large-scale strategic influence operations intended to exacerbate Western societal divisions to induce violence and undermine faith and confidence in national critical industries, such as communications, finance, and energy, and aimed at causing widespread domestic unrest. Additionally, as described in RIAC's analysis concerning MUAI, Russian intelligence services disseminate multiple versions of Western countries' national leadership, making emergency announcements concerning national emergencies and directing the domestic populace to make immediate preparations for crisis, inducing domestic panic, runs on financial institutions, and rushes on food distribution centers and fuel stations. Additionally, Russian intelligence disseminates disinformation claiming that nuclear strikes have occurred in various locations in the West.

Strategic Technical Attack: Russian intelligence services, in collaboration with Russian non-state cyber threat actors, conduct cyberattacks against Western countries' communications, energy, and financial infrastructure, causing widespread and prolonged disruptions or outages. Cyberattacks against communications infrastructure include targeting phone and internet service providers, television and radio stations, government communications, and even HAM radio communications. These attacks are intended to inhibit Western countries from communicating and disseminating information about the reality of the ongoing situation. Cyberattacks against energy infrastructure are intended to reduce or eliminate access to power and the use of utilities. Additionally, cyberattacks against the financial sector are designed to inhibit access to online banking and national critical financial markets.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com