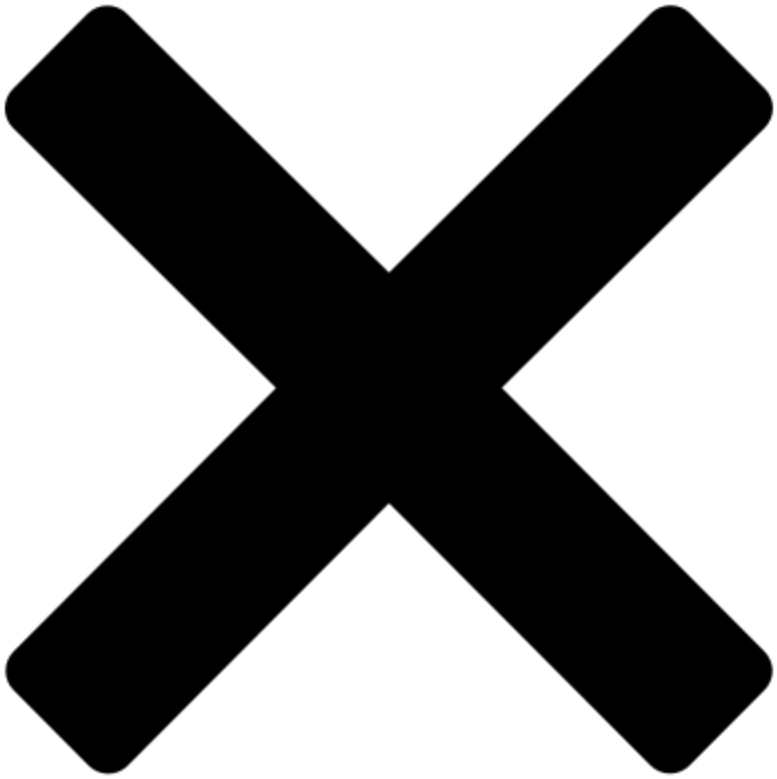
Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan

mandiant.com/resources/blog/cyber-operations-russian-vulkan



As a part of Mandiant's research on Russian cyber and information operations (IO) capabilities, Mandiant worked with a collective of media outlets, including Papertrail Media, Der Spiegel, Le Monde, and Washington Post, to analyze several documents belonging to a Russian IT contractor named NTC Vulkan (Russian: НТЦ Вулкан). The documents detail project requirements contracted with the Russian Ministry of Defense, including in at least one instance for GRU Unit 74455, also known as Sandworm Team. These projects include tools, training programs, and a red team platform for exercising various types of offensive cyber operations, including cyber espionage, IO, and operational technology (OT) attacks.

The documents, which are dated between 2016 and 2020, offer a brief snapshot of previous Russian investments and considerations in scaling cyber operations and capability development. However, Mandiant lacks evidence to prove that the capabilities we discuss

have been implemented or are feasible.

A note on source authenticity: Mandiant cannot conclusively confirm the authenticity of these documents based on limitations in our current visibility. However, we strongly suspect they are legitimate based on consistencies observed across the documents we reviewed, limited instances where we were able to validate details externally, and an apparent alignment between the capabilities detailed for development in these programs and those that we have previously observed used at high levels by Russian intelligence services.

NTC Vulkan Documents Detail Requirements to Develop Cyber and IO Capabilities

NTC Vulkan is a Russian IT contractor based in Moscow, which publicly advertises working on contracts with large companies and government agencies within Russia. The company's website cites compliance with Russian government standards but does not publicly state working with Russian state contractors, such as research institutes or Russian intelligence services. Based on our analysis of the leaked documentation, NTC Vulkan has held contracts with Russian intelligence services on projects to enable cyber and IO operations, potentially in tandem with cyber operations against OT targets.

The documents detail three projects: Scan, Amesit, and Krystal-2B.

Table 1: Summary of main projects identified in NTC Vulkan documents

Tool	Description	Contract Dates
Scan	A comprehensive framework likely used to enable cyber operations. Scan consists of a variety of methods for large-scale data collection and contains comprehensive documentation on how to structure databases to store and handle such information. Based on the signatories, Scan documentation was contracted (at least in part) by GRU Unit 7445, or Sandworm Team.	~2018-2019
Amesit (Alt: Amezit)	A framework used to control the online information environment and manipulate public opinion, enhance psychological operations, and store and organize data for upstream communication of efforts. Information confrontation and psychological operations in Amesit are designed to support IO and OT-related operations.	2016-2018

Krystal-2B	A training platform for exercising coordinated IO/OT attacks against transportation and utility industries using Amesit. The exercise's program highlights particular scenarios against OT environments and Russian infrastructure. Krystal-2B may be a red teaming or defensively focused exercise, but demonstrates interest in coordinating IO/OT attacks.	2018-2020

Cyber Capabilities for Information Confrontation

The cyber operation tools and capabilities detailed in the leaked NTC Vulkan documents are presented as separate and distinct projects. Mandiant did not identify any evidence indicating how or when the tools could be used. However, based on our analysis of the capabilities, we consider it feasible that the projects represent only some pieces of a variety of capabilities pursued by Russian-sponsored actors to conduct different types of cyber operations.

Scan appears to be a comprehensive framework used to gather different types of information such as network details, configurations, and vulnerabilities, among other types of data, to enable cyber operations. Amesit and Krystal-2B focus on developing capability to control the information environment, in part by simulating IT/OT attacks. The documents included pictures of a prototype platform that would enable operators to interact with different cyber operation tools. This combination of capabilities is in line with what Russian intelligence services deem a key part of their information confrontation strategy.

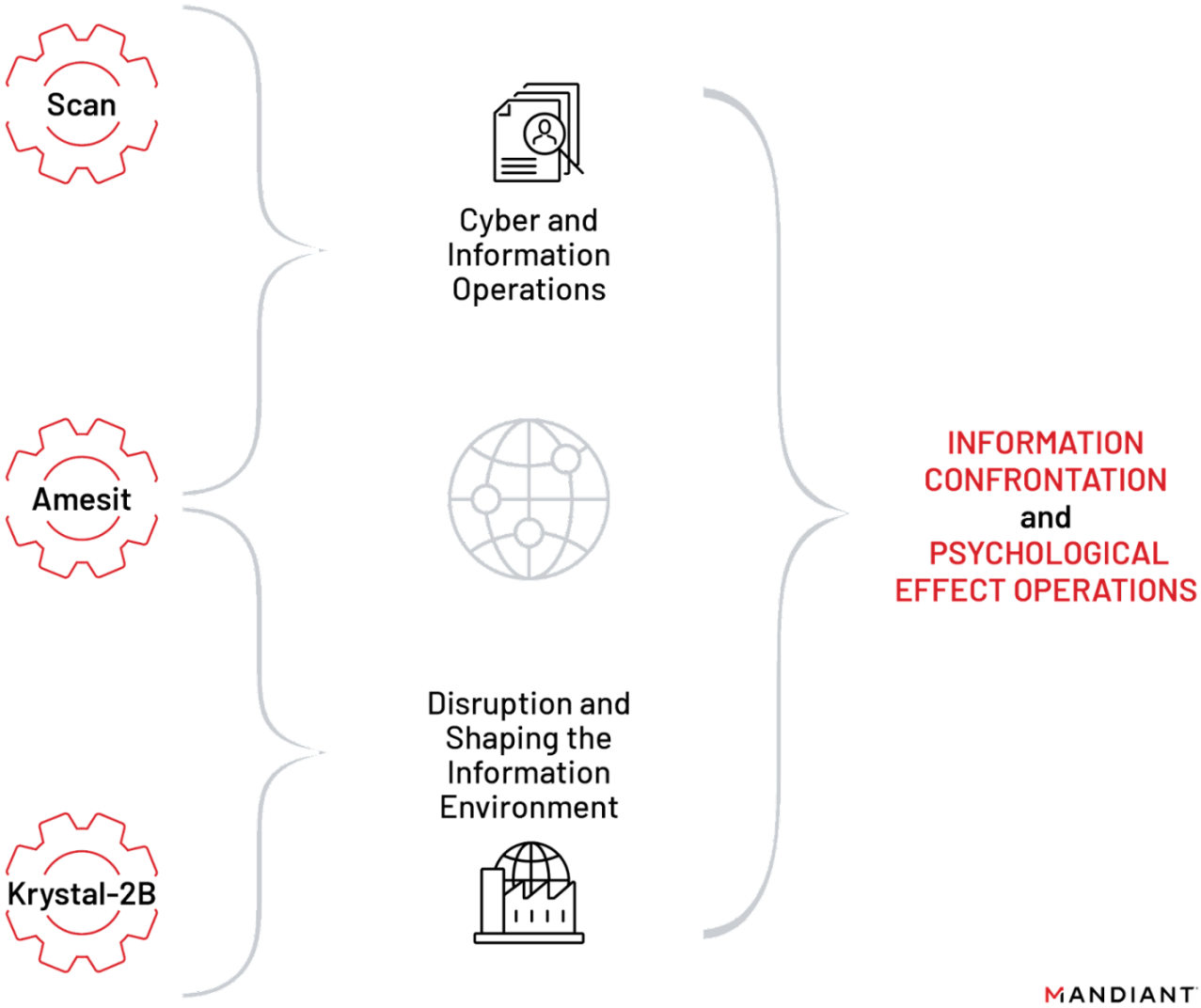


Figure 1: Assessment of capabilities documented in NTC Vulkan aligned with broader strategic goals of Russian intelligence services

Reconnaissance, Preparation, and Enablement of the Attack Lifecycle

Capabilities documented in the contracted NTC Vulkan project Scan could help automate parts of the reconnaissance and preparation of operations. Scan is a framework comprising multiple components including a large-scale database, methods to gather data from various sources, and a platform to process and action such data collections.

The documentation about Scan is incredibly comprehensive, detailing data transfer between components, open-source and foreign-made software and hardware. Additionally, the capabilities described for this tool's design take into consideration the need for coordination across groups and operators in different locations. Comprehensive capability gathering and processing data—such as the one described in Scan—could enable the operators to systematize and automate cyber operations to conduct activity across a range of domains from cyber espionage to OT targeted attacks.

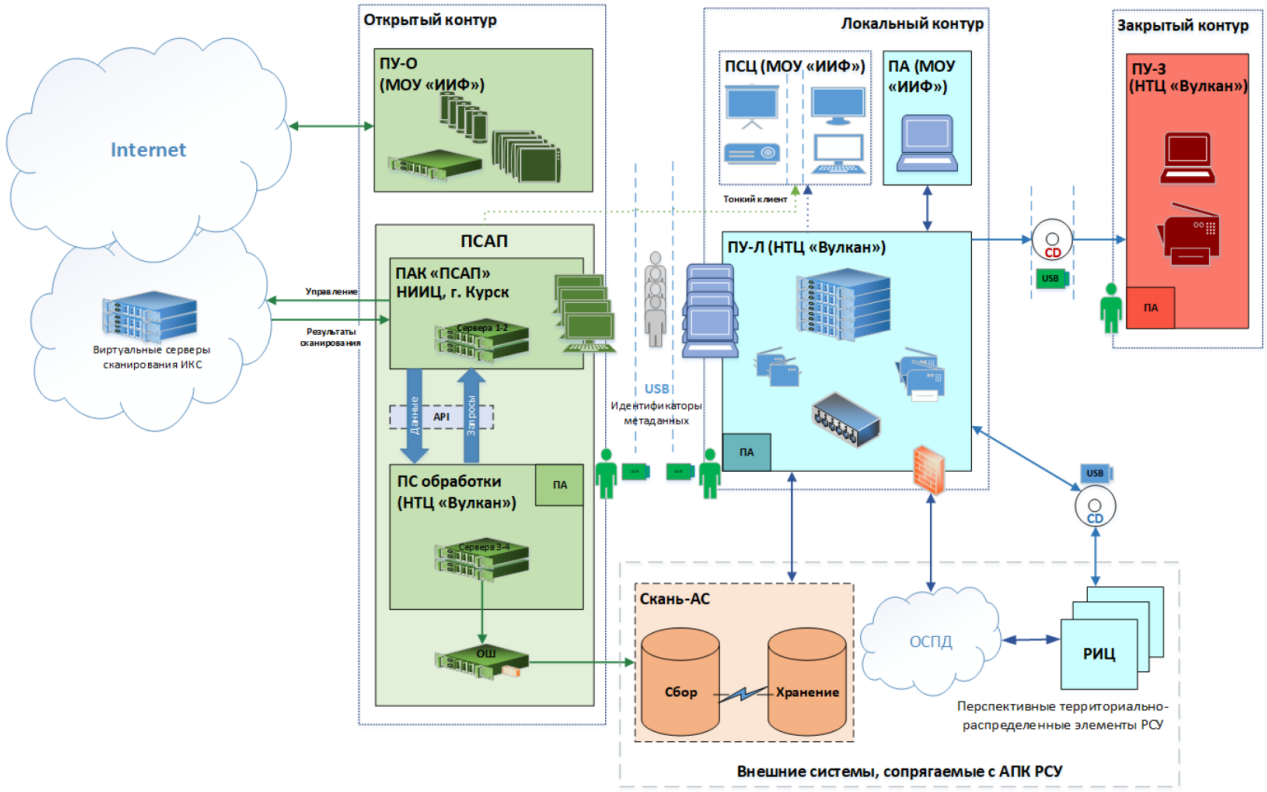


Figure 2: High-level hardware and software specifications associated to the Scan project

- The Scan framework documentation seems to present requirements and initial designs for a database fed by multiple data sources and built for both automated and manual input to enable cyber operations. The documentation provides examples of data collection requirements including, for example, automatic scanning for vulnerabilities, gathering details about network infrastructure, and collecting other relevant information about targets.
- Scan requirements also include enabling operators to collect data manually and via automation. Another requested capability is a “Processing” component, which is manually operated to serve data requests at need.
- Scan requirements also include outlining possible attack paths for operators, visualizing network mappings and target geography. Such capabilities are supposed to be supported by tooling with visualization components and processes for deconfliction across regional units using the framework.

Managing and Executing Information Operations

Capabilities outlined in NTC Vulkan Amesit documentation could support a full information operations life cycle: monitoring the media landscape, creating content to promote a specific narrative, establishing and leveraging means to disseminate that content, and assessing the effectiveness of an operation (Figure 3). The use-case detailed in the documents suggests a systematic approach to IO wherein operators can leverage a suite of options to tailor and adapt their operations.

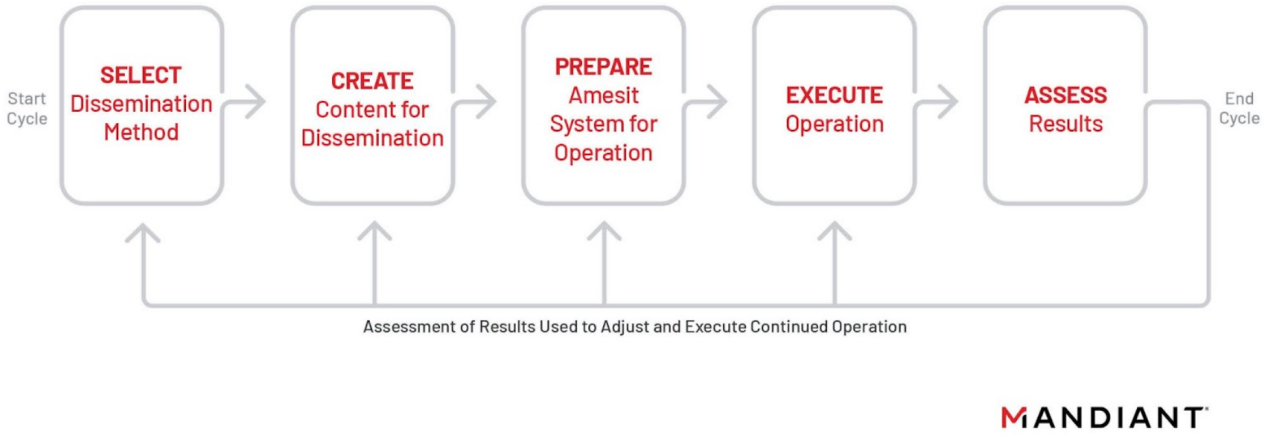


Figure 3: The documents detailing Amesit's functionality outline a specific information operations cycle that the system should support

- Requirements detailed for components of Amesit state that various online forums are "actively used to form and manipulate public opinion" and that an actor interested in manipulating public opinion must be able to identify and leverage the "most effective information channels" to target audiences susceptible to the desired positions.
- Monitoring and collection capabilities include those that appear intended to enable operators to track the promotion of a given narrative or issue across various segments of the online discussion, including on news portals, social media, blogs, and forums.
- Content creation requirements would allow operators to create or modify so-called "special materials" for dissemination in operations. This includes text, image, video, and audio content in various formats.
- Means to disseminate content across multiple vectors are specified, including via social media and blogs, SMS text messaging, and email.

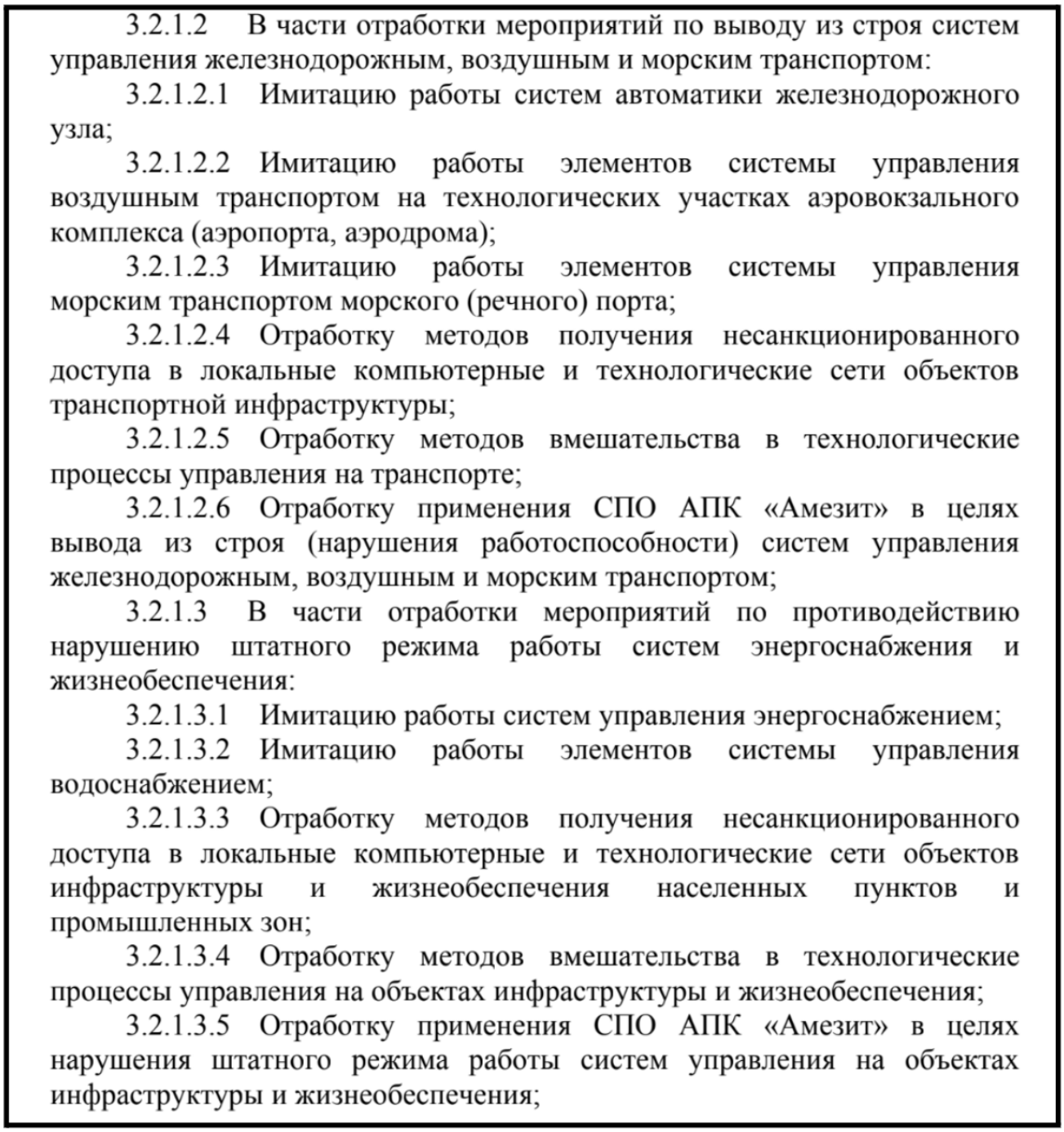
    An individual operator should be able to manage at least 100 social media profiles from their workstation, according to the requirements.

The requirements also discuss how to reduce the risk of identification and potential attribution. This includes the ability to clean and replace metadata attached to the files of content created for dissemination, and means of creating inauthentic profiles on social media and forums for content promotion.

Functions detailed in the requirements also account for the ability to localize the targeting of an operation within a given geographic area. While it is unclear what targets the tools would be used upon, some of the social media platforms and information resources listed as targets for data collection and content dissemination include those more specific to Russia and the surrounding region. It also includes those with broader global usership, suggesting that Amnesit tooling could be used both for regional or broader targeting.

Targeting Operational Technology Systems

The documents from NTC Vulkan also include contents related to OT systems in two projects: Krystal-2B and Amesit. Krystal-2B is a training platform that simulates OT attacks against different types of OT environments in coordination with some IO components by leveraging Amesit "for the purpose of disruption." The Krystal-2B documentation highlights scenarios against Russian military infrastructure, rail systems, airports, sea ports, and energy and water utilities, but does not detail specific methodologies on the malicious activities executed within these exercises. Krystal-2B appears designed to support both offensive exercises against OT environments (Figure 4) and defensive exercises to examine vulnerabilities in Russian military infrastructure.



3.2.1.2 В части отработки мероприятий по выводу из строя систем управления железнодорожным, воздушным и морским транспортом:

3.2.1.2.1 Имитацию работы систем автоматики железнодорожного узла;

3.2.1.2.2 Имитацию работы элементов системы управления воздушным транспортом на технологических участках аэровокзального комплекса (аэропорта, аэродрома);

3.2.1.2.3 Имитацию работы элементов системы управления морским транспортом морского (речного) порта;

3.2.1.2.4 Отработку методов получения несанкционированного доступа в локальные компьютерные и технологические сети объектов транспортной инфраструктуры;

3.2.1.2.5 Отработку методов вмешательства в технологические процессы управления на транспорте;

3.2.1.2.6 Отработку применения СПО АПК «Амезит» в целях вывода из строя (нарушения работоспособности) систем управления железнодорожным, воздушным и морским транспортом;

3.2.1.3 В части отработки мероприятий по противодействию нарушению штатного режима работы систем энергоснабжения и жизнеобеспечения:

3.2.1.3.1 Имитацию работы систем управления энергоснабжением;

3.2.1.3.2 Имитацию работы элементов системы управления водоснабжением;

3.2.1.3.3 Отработку методов получения несанкционированного доступа в локальные компьютерные и технологические сети объектов инфраструктуры и жизнеобеспечения населенных пунктов и промышленных зон;

3.2.1.3.4 Отработку методов вмешательства в технологические процессы управления на объектах инфраструктуры и жизнеобеспечения;

3.2.1.3.5 Отработку применения СПО АПК «Амезит» в целях нарушения штатного режима работы систем управления на объектах инфраструктуры и жизнеобеспечения;

Figure 4: Sample excerpt of Krystal-2B program highlighting training for OT-oriented cyber

attacks
The Krystal-2B project relies on tooling from another project named Amesit. The OT portion of the project is referenced in a set of testing requirements for Amesit, which describes the implementation of simulated OT test bed environments for rail and pipeline control systems. The Amesit documentation indicates these models would be supported by either graphical or physical models of these systems to visualize the effects of cyber attacks, clearly establishing these industries as Russia's targets of interest for OT-oriented attacks.

The only attack-related requirement for the OT test beds is that they provide "simulation of ARP-spoofing attacks, leading to violations of simulated technological processes." These violations include either common IT-oriented impacts on the network infrastructure or complex changes in the parameters of the OT via "specialized software." It is unclear whether such software refers to Amesit tooling, legitimate programmable logic controller (PLC) engineering software, or some other existing capabilities. While we have not linked this activity to existing toolsets, frameworks like INCONTROLLER are designed to support these types of parameter changes.

The document also specifies specific parameters of the control systems that the attacker should be able to affect and physical impacts the attacker should be able to generate. These specifications provide potential insight into the process-level design of these attack scenarios.

- For rail systems, this includes manipulating the speed of trains, creating unauthorized track transfers, causing car traffic barriers to fail, and causing combined heat and power (CHP) units to fail, with the explicit objective of causing train collisions and accidents.
- For pipeline systems, this includes closing valves, shutting down pumps, overfilling tanks, spilling materials, and causing pump cavitation and overheating.

Although there is little information in both documents on how the attacks would occur in a real setting, the capabilities we observed are consistent to those Mandiant has observed in previous attacks and tooling from Russian-sponsored actors. Another noteworthy observation is the incorporation of IO capabilities in the same projects that describe OT targeting, which hints at the likelihood of deploying campaigns that leverage both resources to support complex information warfare operations.

Takeaways

The contracted projects from NTC Vulkan provide insight into the investment of Russian intelligence services into developing capabilities to deploy more efficient operations within the beginning of the attack lifecycle, a piece of operations often hidden from our view. A framework like the one suggested in the Scan project illustrates how the GRU may be trying

to enable fast-paced operations with high coordination among regional units. A once-segmented GRU cyber operation may become streamlined and more efficient using a framework like Scan.

These projects also show interest in holistic operations to conduct information control and/or confrontation and amplify the psychological effects of cyber operations. For example, Amesit and Krystal-2B demonstrate a high value placed on the psychological impact of offensive cyber attacks, specifically OT operations, by highlighting the role of information operations in determining the impact of an ICS incident. The combination of different tactics in cyber operations is familiar to Russian cyber operations: an early example is the multifaceted BLACKENERGY operation in 2015 leading to disruption of energy infrastructure in Ukraine. We have also seen the combination of IO and disruptive cyberattacks throughout the Ukraine war.

The documentation from Krystal-2B and Amesit also displays interest in critical infrastructure targets, particularly energy utilities and oil and gas, but also water utilities and transportation systems, including rail, sea, and air. As we continue to observe the intensification of threat activity from Russian-sponsored actors in parallel to the invasion in Ukraine, defenders should remain aware about the capabilities and priorities reflected in these documents to be prepared for protecting critical infrastructure and services.