RE: PDNCD-013023-002 Due by Feb 6 at 2:00 pm - Chamber Cyber Salon Dinner

From: "Scheidler, Joe W. EOP/NCD" (b) (6)
To: "Klein, Julie G. EOP/NCD" (b) (6), "Chang, Caroline EOP/NCD" (b) (6), "Berlin, Jen S. EOP/NCD" <(b) (6)
Cc: "Ring, Haley A. EOP/NCD" (b) (6), "Leiserson, Nick J. EOP/NCD" <(b) (6), "Krejsa, Harry H. EOP/NCD" <(b) (6), DL ExecSec (b) (6), ONCD Stakeholder Engagement (b) (6)
Bcc: "Hochman, Michael C. EOP/NCD" <(b) (6)
Date: Tue, 07 Feb 2023 12:06:10 -0500
Attachments: Event Memo - Commerce Cyber Salon Dinner - redlines.docx (78.78 kB)

HI team,

Thanks for the nice prep on this one – attaching minor cosmetic redlines and will include a clean copy in the PDNCD book tonight.

VR,
Joe

From: Klein, Julie G. EOP/NCD <(b) (6)
Sent: Monday, January 30, 2023 6:12 PM
To: Chang, Caroline EOP/NCD (b) (6); Berlin, Jen S. EOP/NCD (b) (6)
Cc: Ring, Haley A. EOP/NCD <(b) (6); Leiserson, Nick J. EOP/NCD (b) (6); Krejsa, Harry H. EOP/NCD <(b) (6); DL ExecSec (b) (6); ONCD Stakeholder Engagement <(b) (6)
Subject: RE: PDNCD-013023-002 Due by Feb 6 at 2:00 pm - Chamber Cyber Salon Dinner

Yes, thanks.

Jen, let's connect and discuss topics that need TPs. Is there a theme to the dinner?

From: Chang, Caroline EOP/NCD <(b) (6)
Sent: Monday, January 30, 2023 12:38 PM
To: Berlin, Jen S. EOP/NCD (b) (6); Klein, Julie G. EOP/NCD <(b) (6)
Cc: Ring, Haley A. EOP/NCD (b) (6); Leiserson, Nick J. EOP/NCD (b) (6); Krejsa, Harry H. EOP/NCD <(b) (6); DL ExecSec (b) (6); ONCD Stakeholder Engagement (b) (6)
Subject: PDNCD-013023-002 Due by Feb 6 at 2:00 pm - Chamber Cyber Salon Dinner

Dear Jen and Julie,

As discussed, in advance of PDNCD's Chamber of Commerce Cyber Salon Dinner, can you please work with Nick and Harry's team to prepare an event memo? Email traffic is included in the link.

Best,
Caroline

GENERAL INFORMATION

Name:	Chamber of Commerce Cyber Salon Dinner		
Int. Due Date:	2:00 pm, Feb 6	**ID:**	013023-002
Event Date:	Feb 8	**Routing:**	PDNCD Book
Assigned to:	Jen, Julie	**Type:**	Event Memo

NOTES AND DOCUMENT DETAILS

Document(s):	Document Location

COORDINATION AND REVIEW

Req. Coord:	Harry, Nick
FO Clearance:	N/A
Legal Review:	N/A
Clearance:	ExecSec

Caroline Chang
Senior Advisor to NCD and ExecSec
Office of the National Cyber Director
Executive Office of the President
(b) (6) [redacted]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

EVENT MEMORANDUM

PRINCIPAL DEPUTY NATIONAL CYBER DIRECTOR
REMARKS AT U.S. CHAMBER OF COMMERCE CYBER SALON DINNER

DATE: February 8, 2023

EVENT TIME: 6:00-8:00pm

DEPARTURE: 5:55pm

LOCATION: U.S. Chamber of Commerce, Meeting Room 3/4, 1615 H Street, NW

EVENT TYPE: Off-the-record, cyber salon dinner

ROLE: Featured Guest

HOST: U.S. Chamber of Commerce

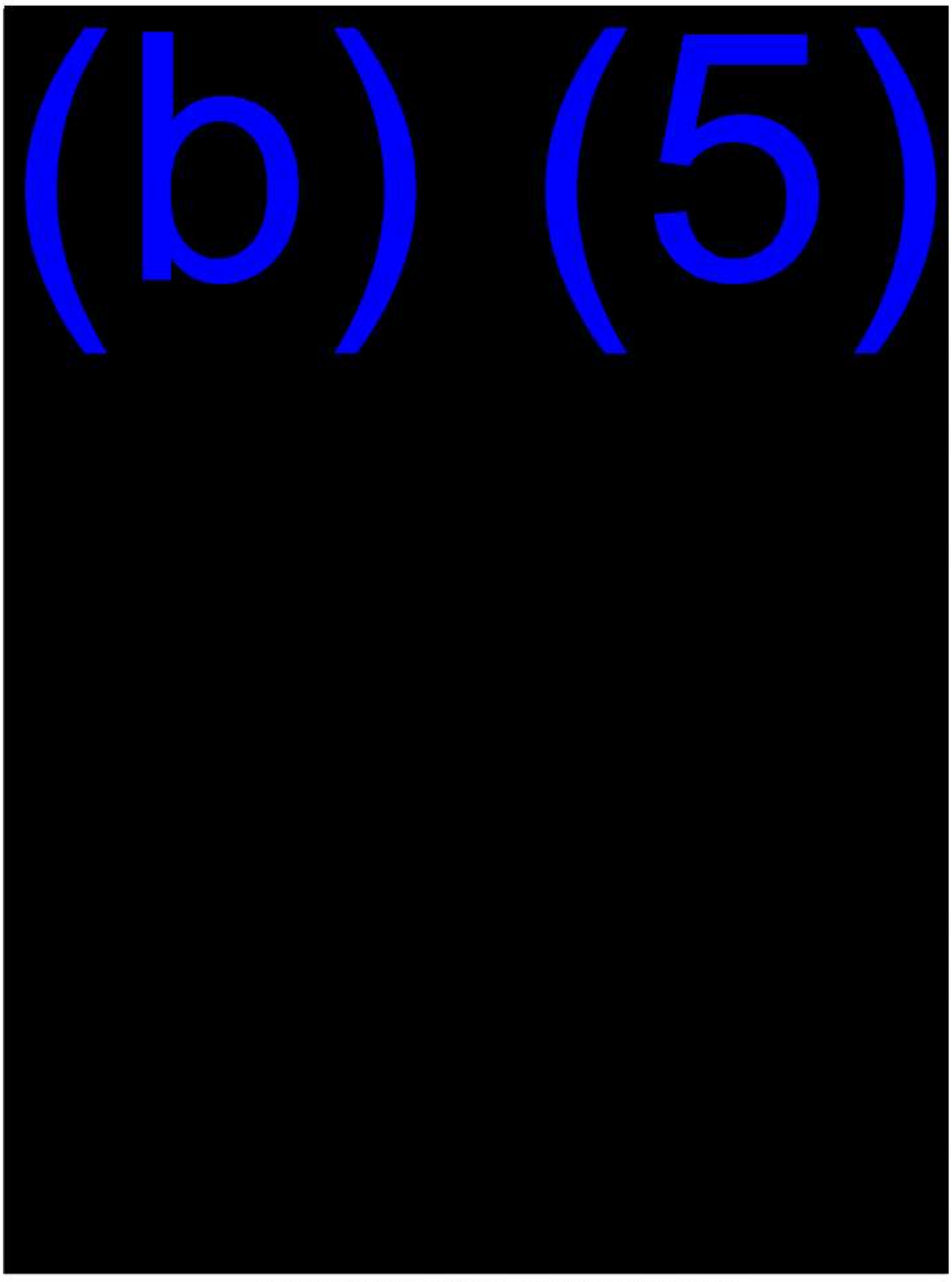
ONCD STAFF: Jen Berlin, ANCD Stakeholder Engagement (not attending)

EVENT POCs:

Chris Roberti, senior vice president, (b) (6)
Vince Voci, vice president, (b) (6)
Lauren Anderson, coordinator, (b) (6)

[APG]

UNCLASSIFIED//FOR OFFICIAL USE ONLY


(b) (5)

Chris the invitation to be a part of this new event, give a nod to our USG counterparts who are also participating, and thank the many members of the audience whose feedback and ideas were essential to the development of the strategy.

The following discussion topics were provided to all dinner participants. These issues are meant to inform the discussion—but it will not be scripted and the conversation will likely end up covering only a few topics (and participants may organically inject issues not listed).

Chamber's suggested topics:

- NCS
    - Critical infrastructure cybersecurity
        - Regulatory framework (between federal and states and between the U.S. and its allies)
        - Regulatory harmonization
        - Public private partnerships and operational collaboration
    - Risk and consequence operations
        - Defend forward, persistent engagement, and law enforcement collaboration
    - IoT security and software liability
    - International cybersecurity and critical emerging technology
        - International cyber assistant fund
- Cyber incident reporting and public disclosure
- Corporate cyber sustainability
- Cyber investment workforce
- EO 14028 implementation/zero trust
- Privacy
- Supply chain security

V. DISCUSSION POINTS [OR QUESTIONS]:

ONCD's Top Cyber Priorities:

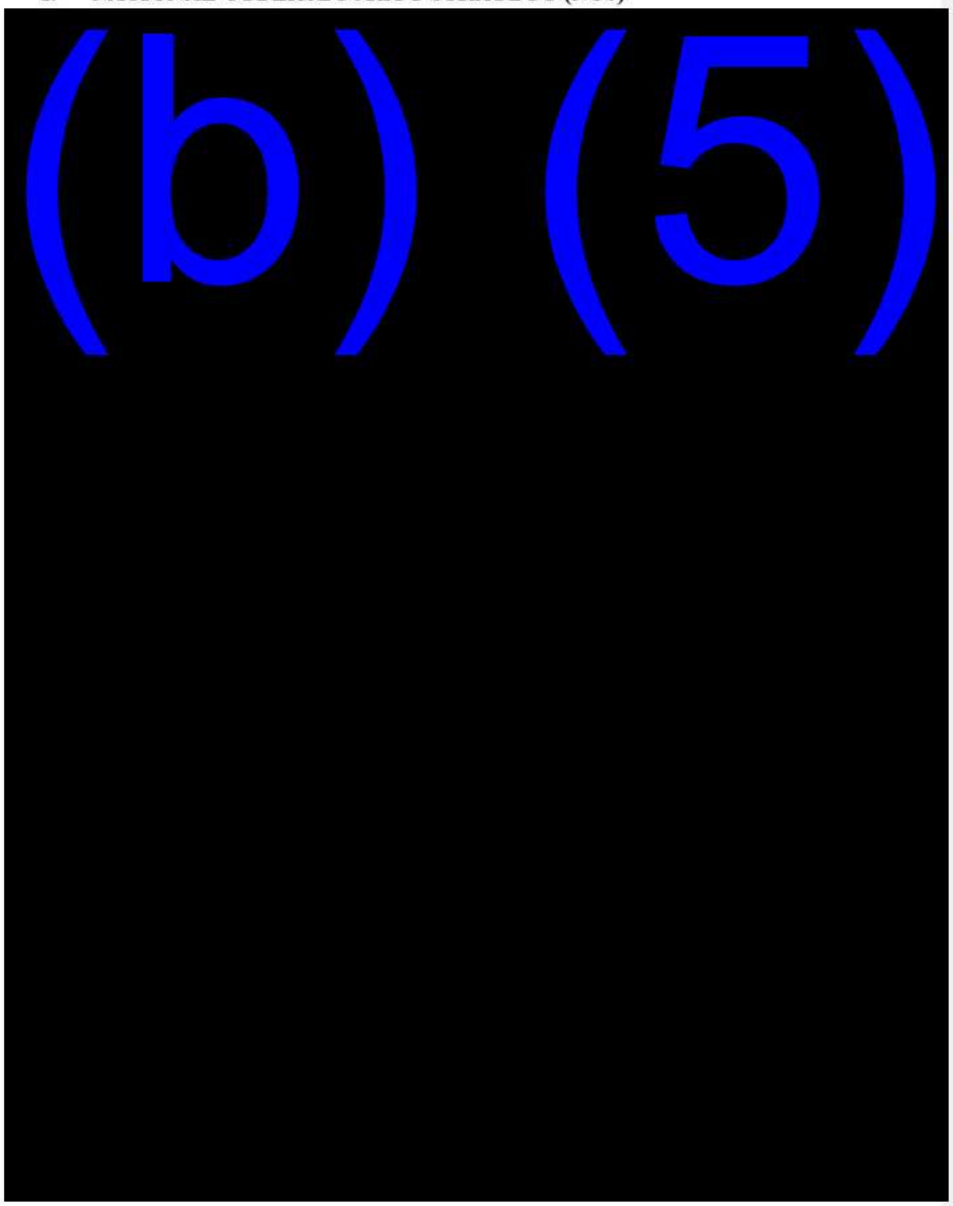
1. National Cybersecurity Strategy
2. Cyber Investment
3. Regulation Harmonization
4. Workforce
5. EO 14028 Implementation and Zero Trust

Additional Cyber topics that participants might raise:

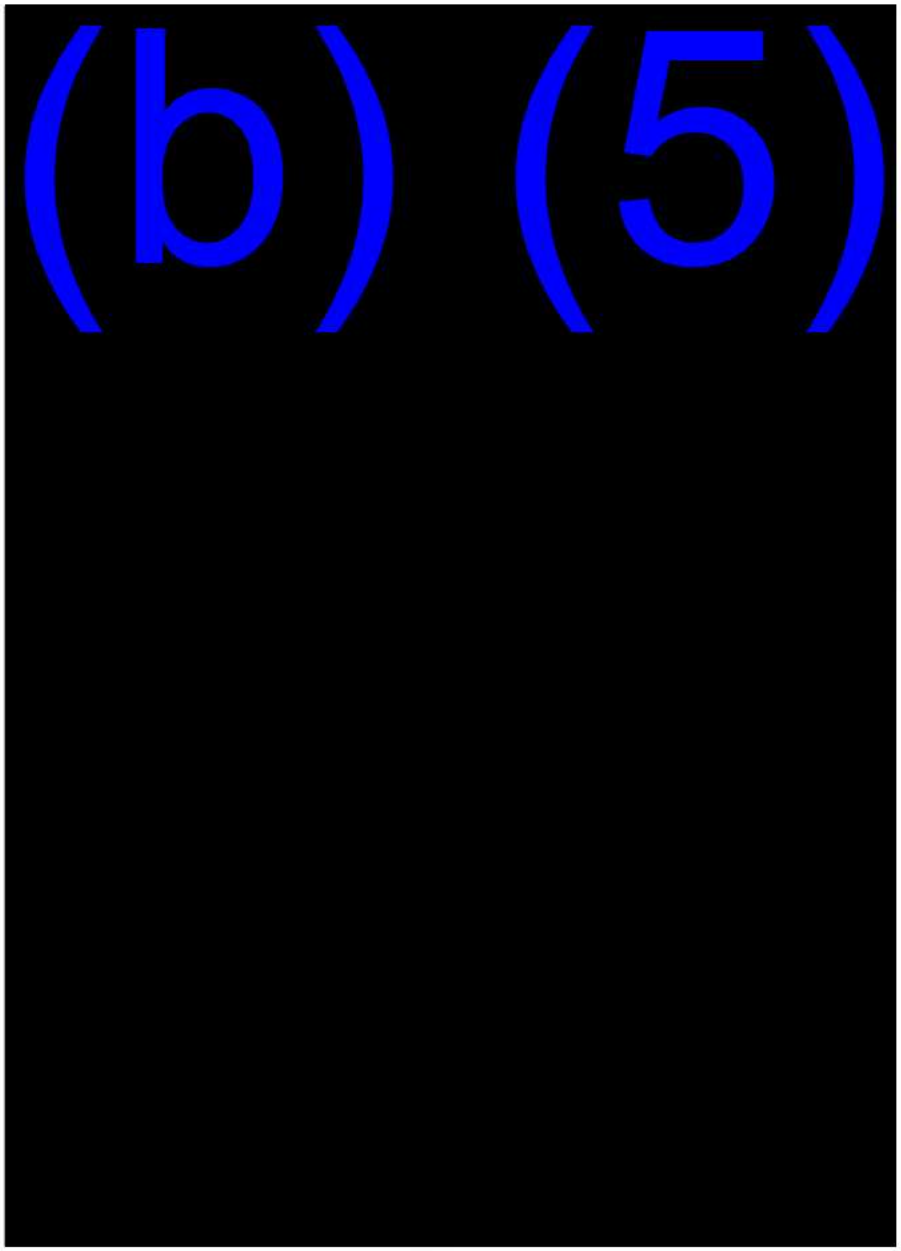
- Regulation
- Privacy
- Know Your Customer (KYC) EO
- Encryption/Going Dark
- TikTok

[APG]

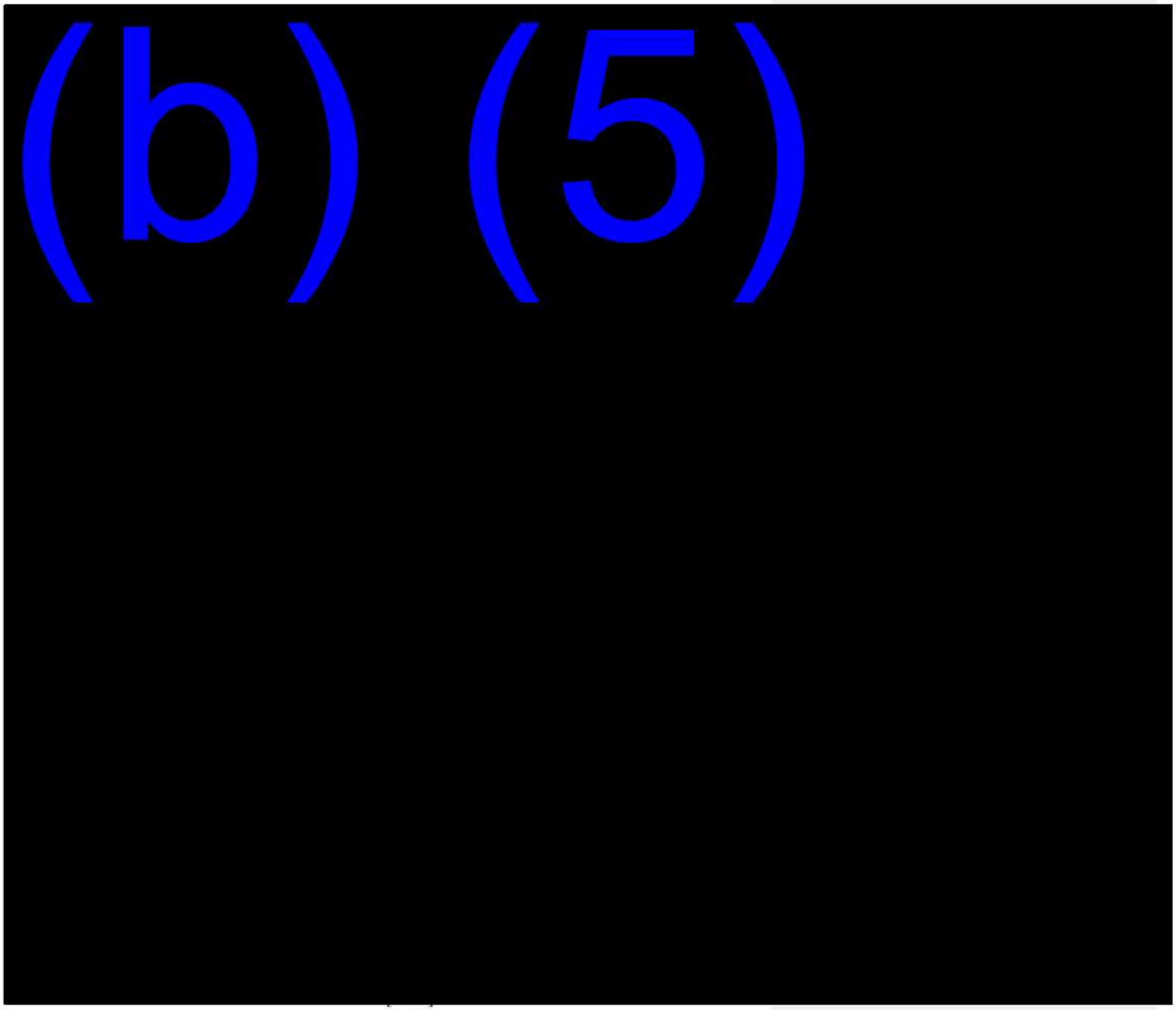
I. NATIONAL CYBERSECURITY STRATEGY (NCS)

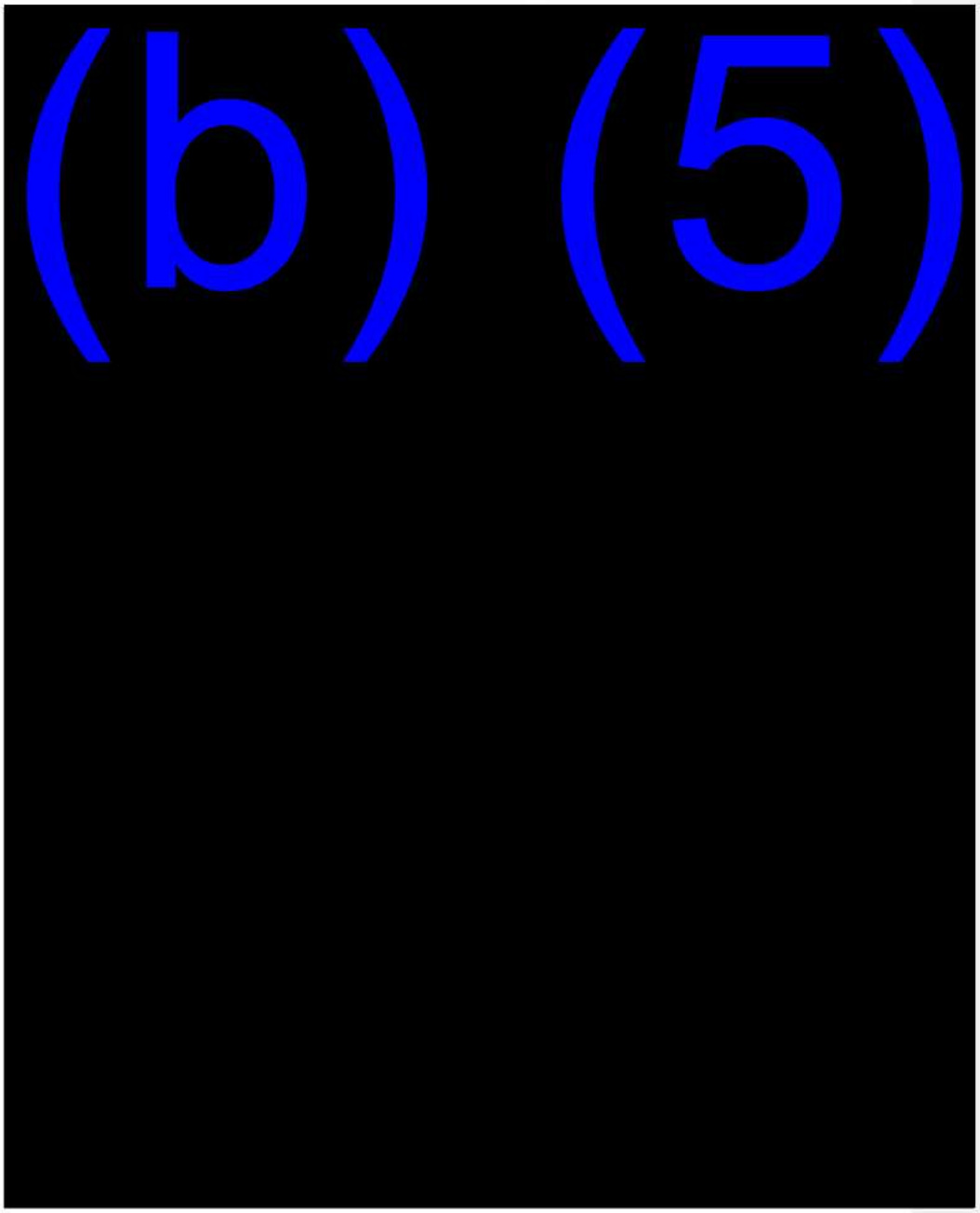


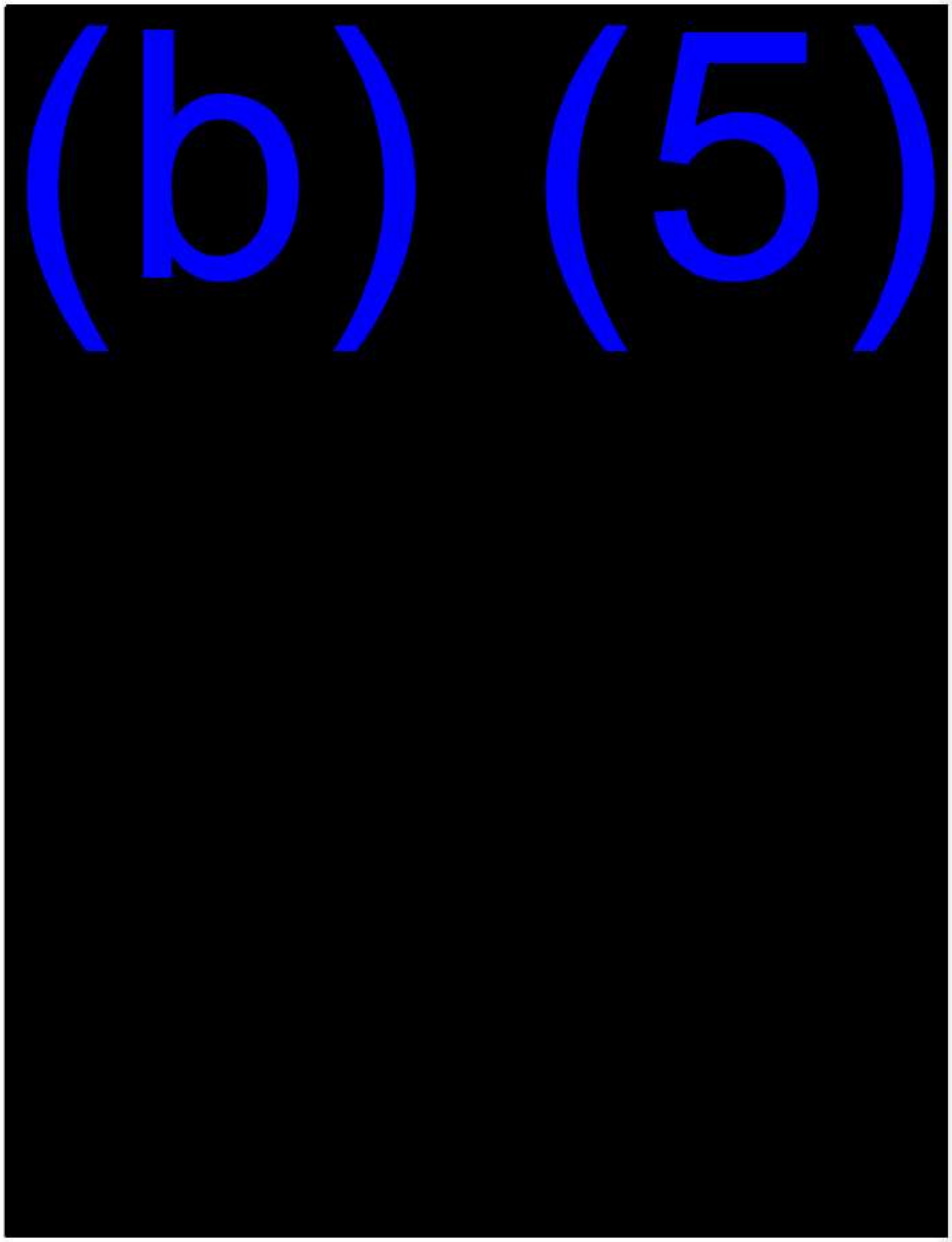
[APG]



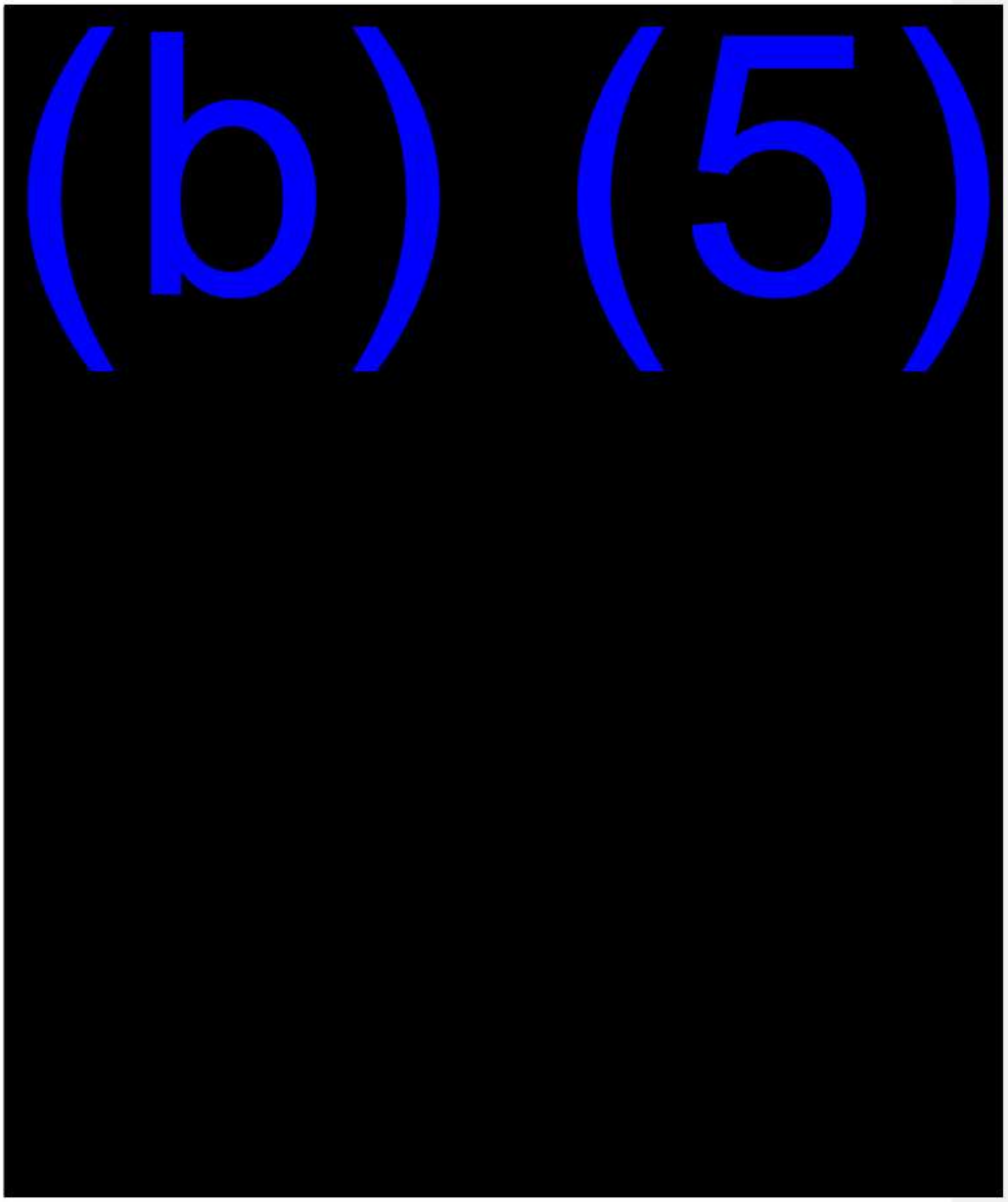
[APG]


(b) (5)

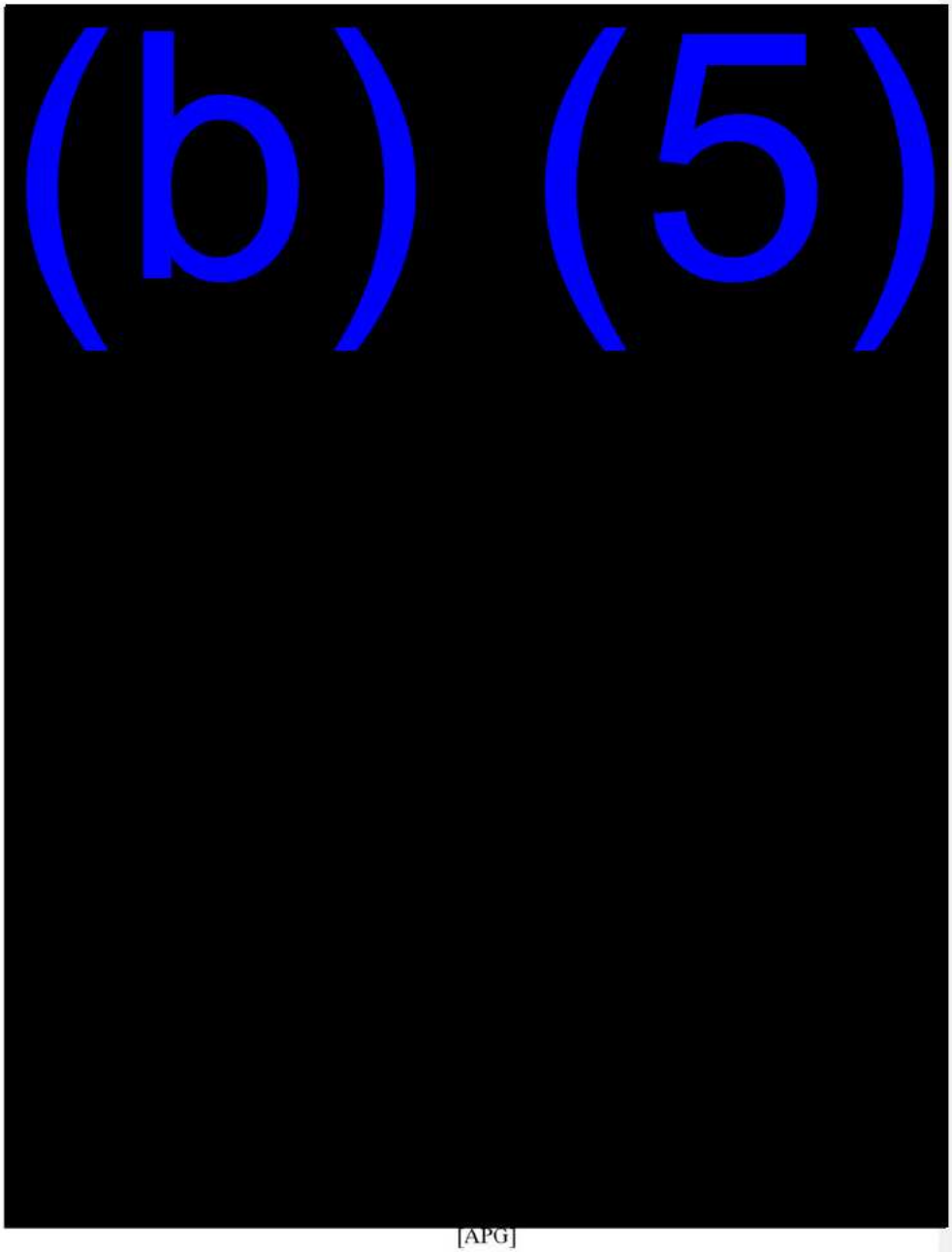

(b) (5)



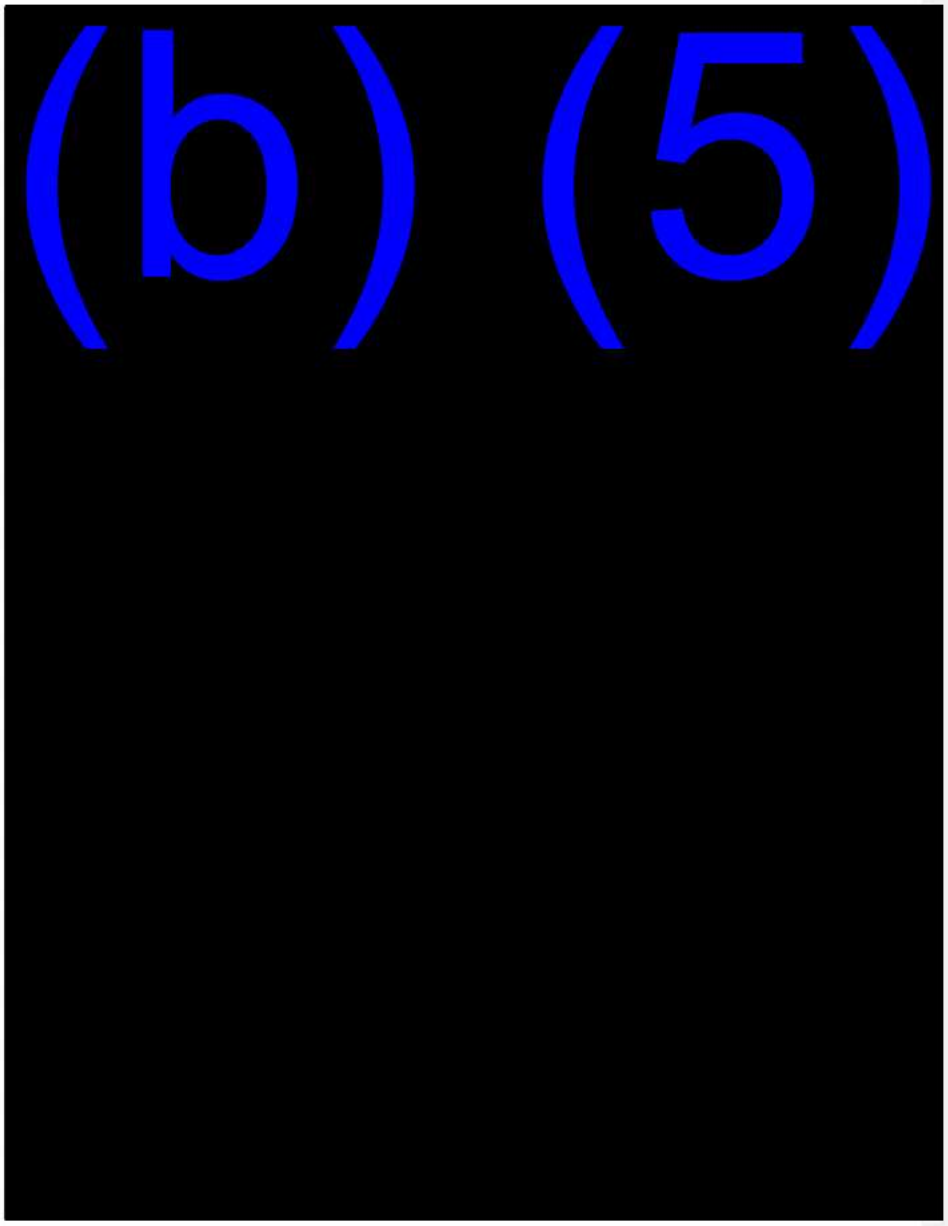
[APG]



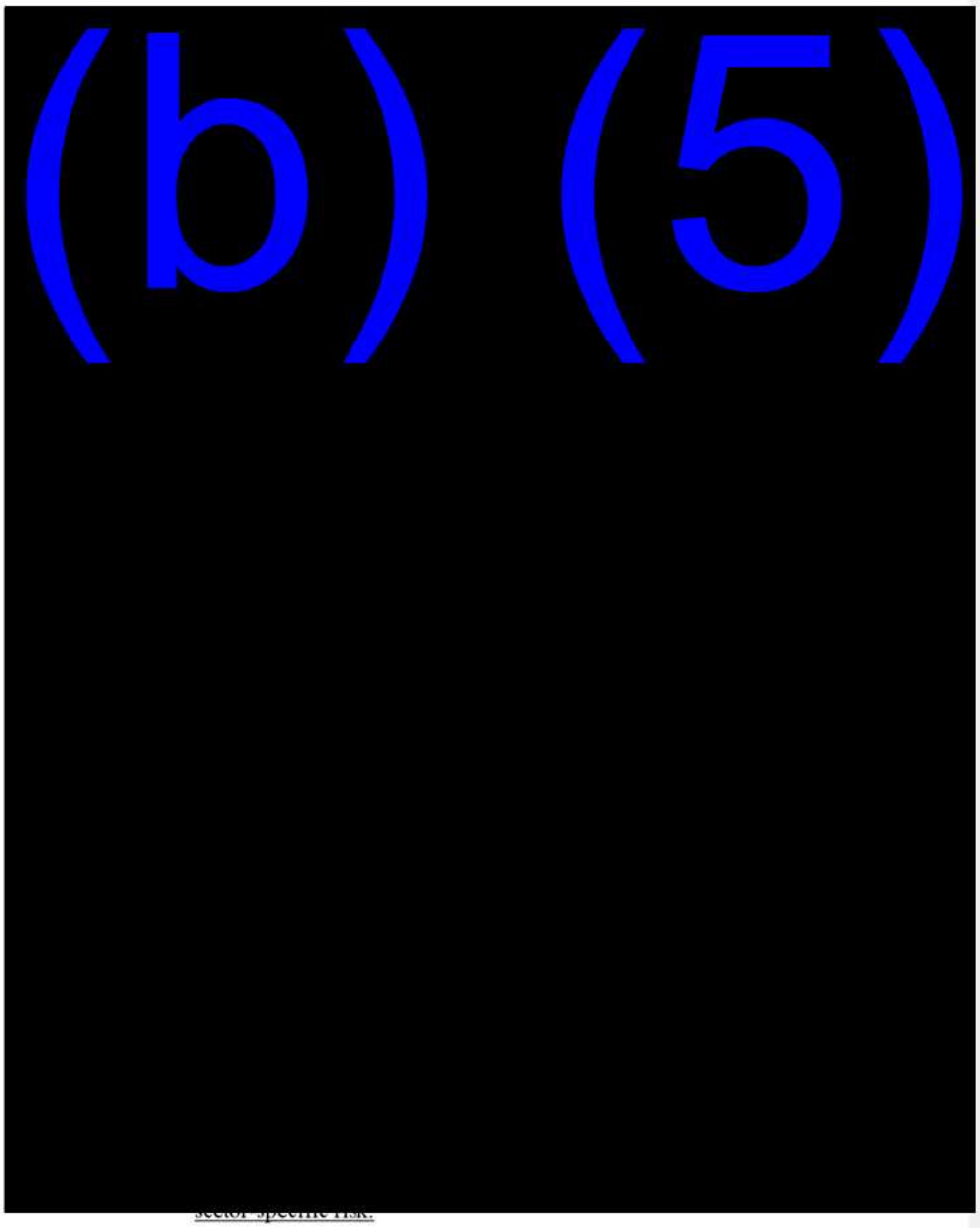
[APG]



[APG]

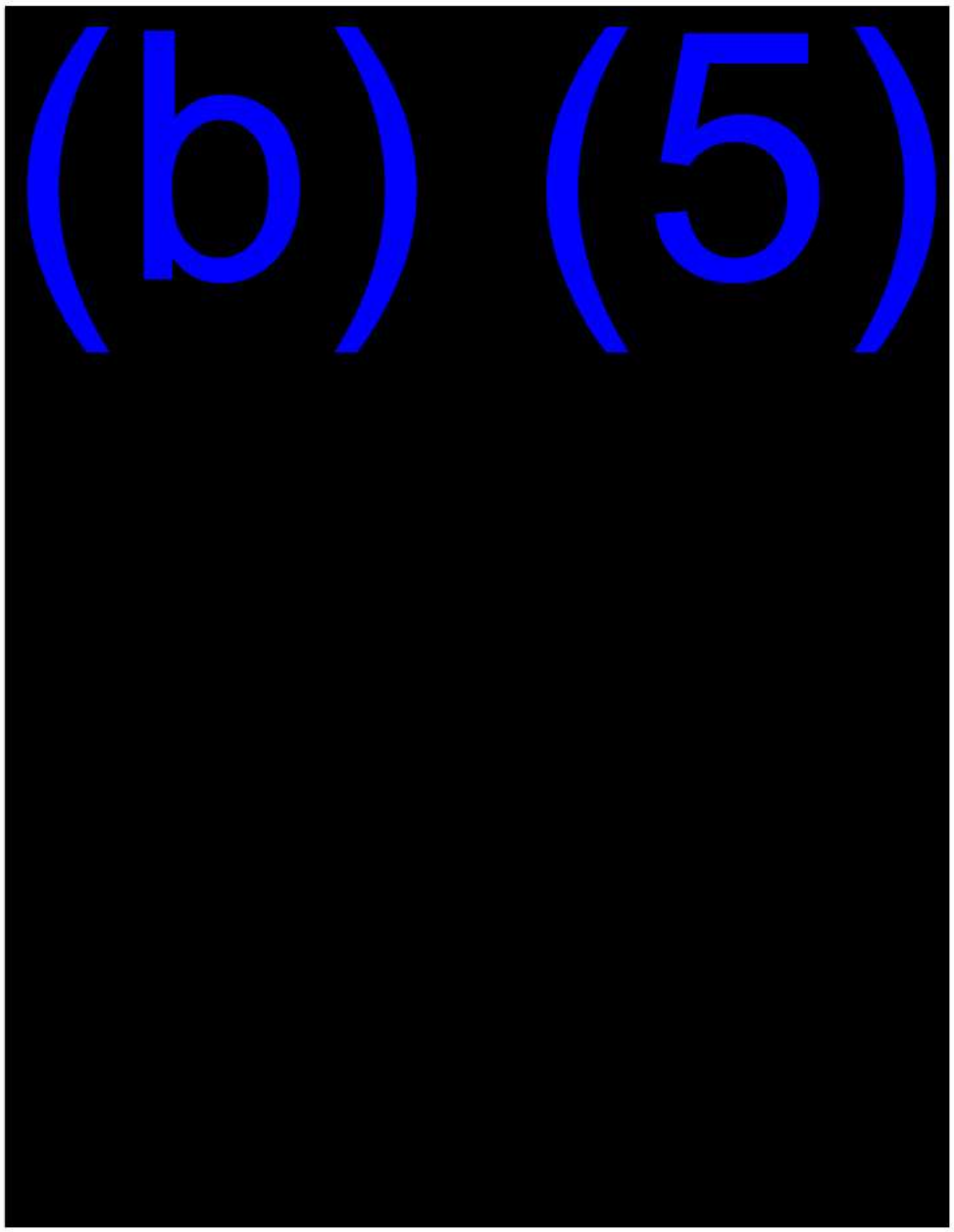


[APG]

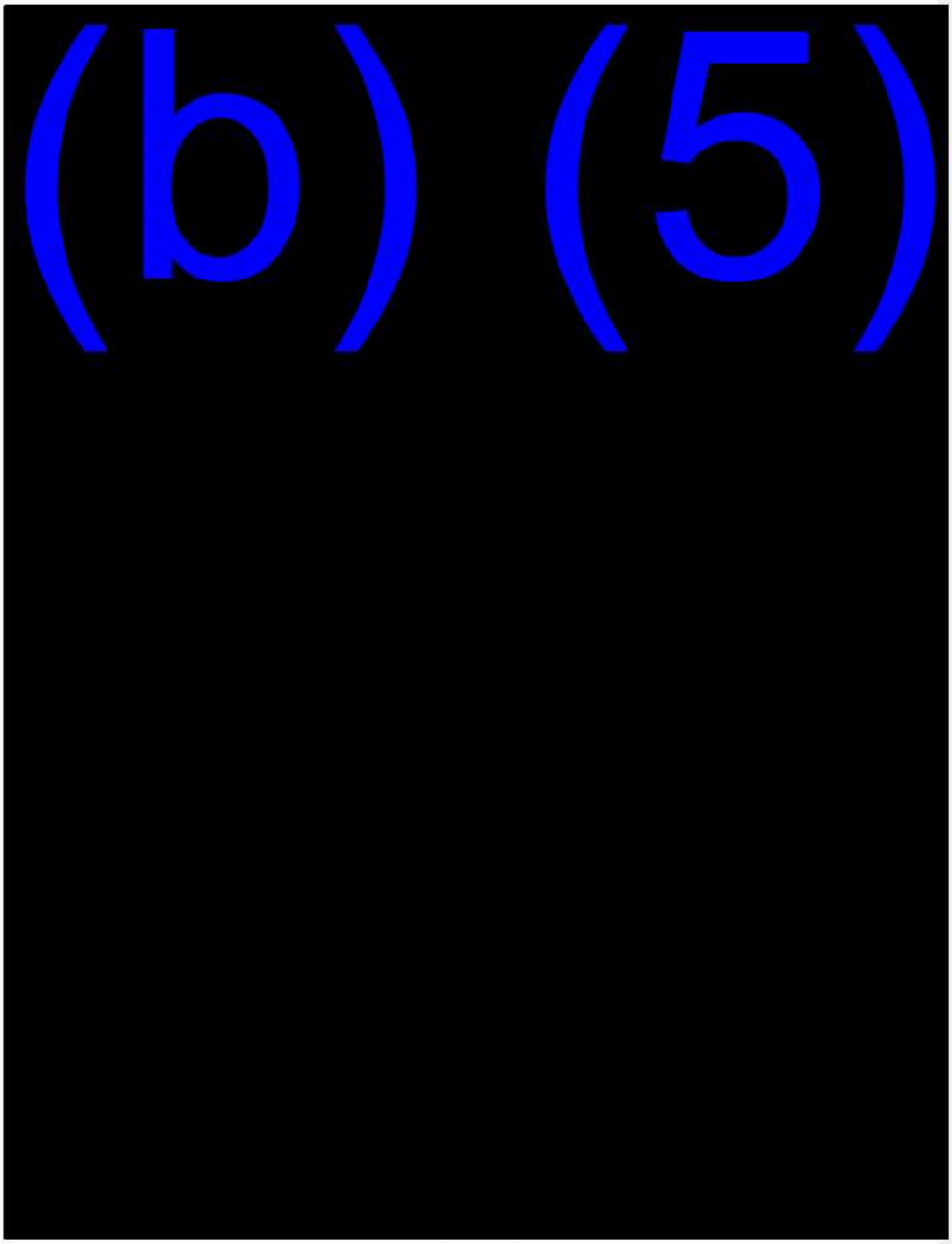


sector-specific risk.

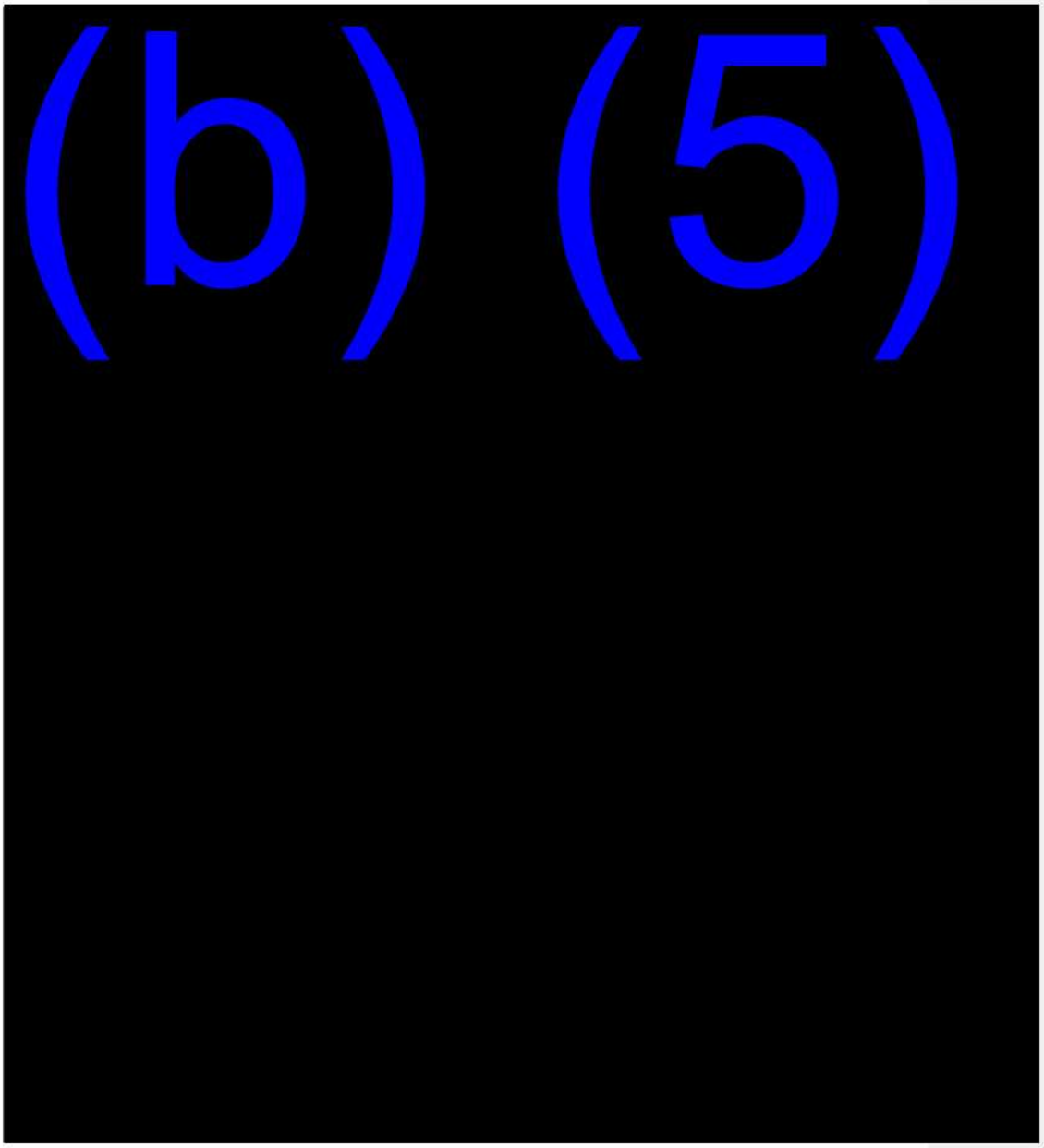
[APG]



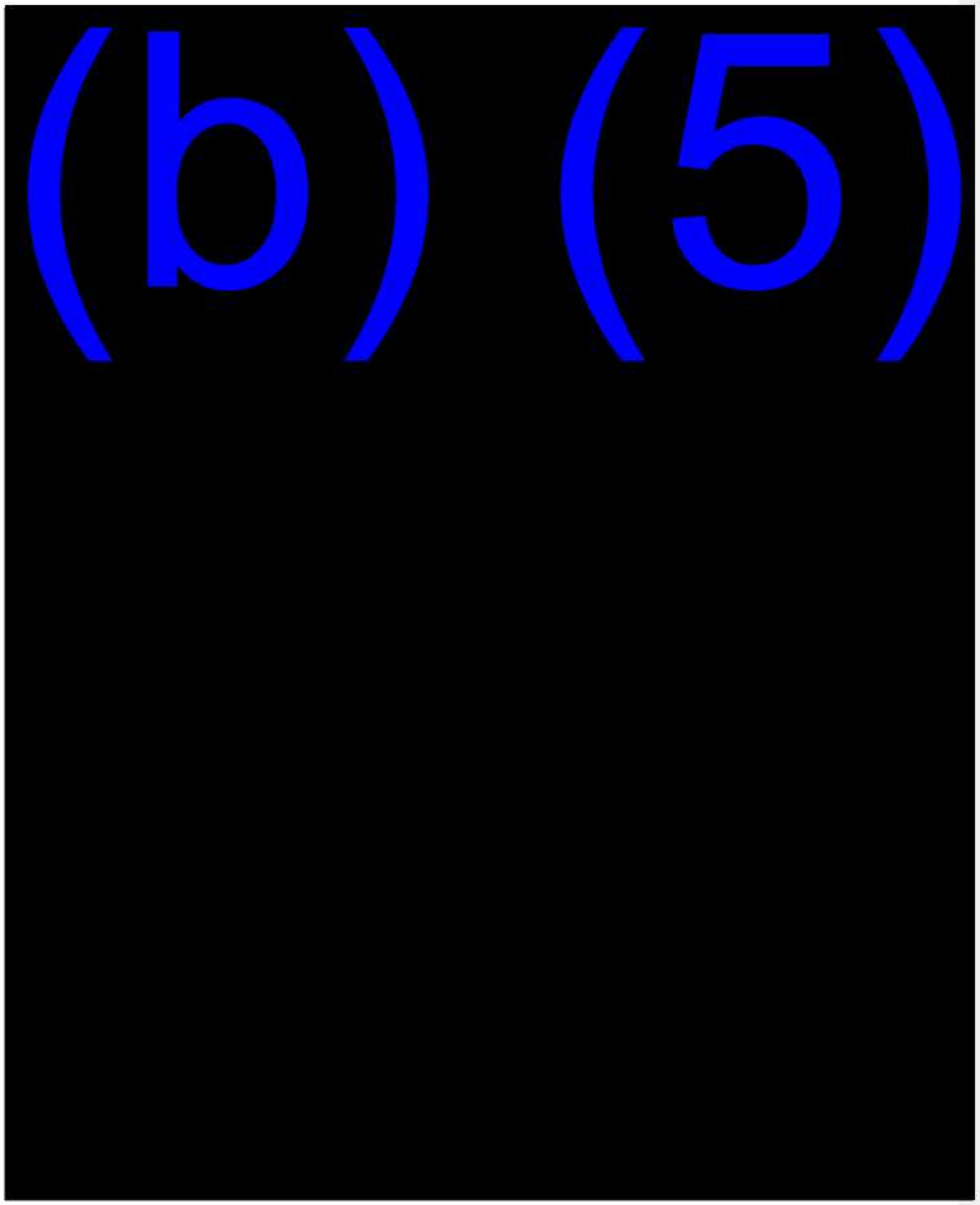
[APG]



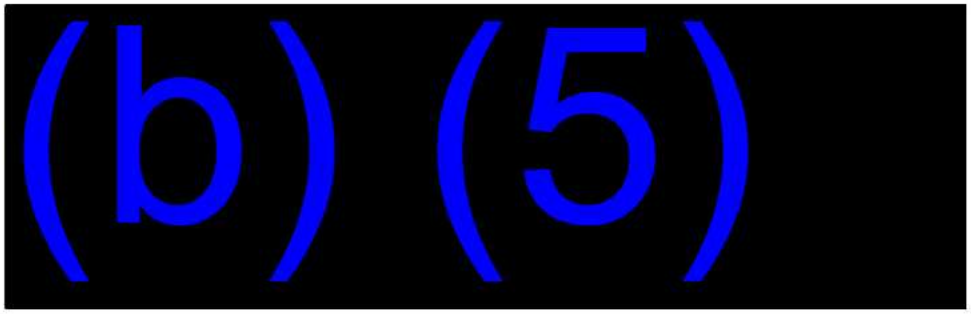
[APG]



[APG]



[APG]



[APG]

[AD]

OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE SECRETARY

Tracking

NUMBER: **013023-002**
VERSION: **v(1.2)**
DATE: **07 February 2023**

Coordination and Approval

PREPARED BY: Jen Berlin, (b) (6)
Julie Klein, (b) (6)

CLEARED BY: Joe Scheidler, Special Advisor, ExecSec

Documents

APPENDICES: Appendix A: Read-ahead Material from the U.S. Chamber of Commerce
Appendix B: Printouts of Referenced Articles

[APG]

RE: CISA/ONCD/OMB Monthly Sync

From: "Barr, Lisa N. EOP/NCD" (b) (6)

To: CSD Executive Assistant Director Scheduler (b) (6), "Dudley, Drenan E. EOP/NCD" <(b) (6), "Goldstein, Eric (He/Him)" (b) (6), "Hartman, Matthew (He/Him)" (b) (6), "Duffy, Michael" <(b) (6), "Herckis, Mitch D. EOP/OMB" <(b) (6), "Higgins, Neal L. EOP/NCD" (b) (6), "DeRusha, Chris J. EOP/OMB" <(b) (6), "Mill, Eric R. EOP/OMB" (b) (6), "Beckel, Sarah" <(b) (6), "Romans, Clayton" (b) (6), "Roebuck, Jermaine (He/Him)" <, "Gross, Martin" <(b) (6), "Yuhasz, Amy" (b) (6), "Conley, Alyson (She/Her)" <(b) (6), "Hartsook, Shelly" <(b) (6), "Mergen, Margaret C. EOP/OMB" (b) (6), "Abrams, Andrew D. EOP/OMB" <(b) (6), "Butera, Christopher (He/Him)" (b) (6), "Polk, Nick J. EOP/OMB" (b) (6), "Muniz Rodriguez, Christian A. EOP/NCD" (b) (6), "Radesky, Sandra (She/Her)" (b) (6), "Thompson, Robert" (b) (6), "Gazlay, Jay (He/Him)" (b) (6), "LYUBLANOVITS, SHONDREA" (b) (6), "Shaw, Robert" (b) (6), "Bokan, Branko" <, "Isaac, Kim" (b) (6), "Bowen, Ethan" <(b) (6), "Petrianni, Peter" <(b) (6), "Cohen, Natasha" (b) (6)

Cc: "Olamide, Simisola (CTR)" <(b) (6), "Mireles-Beuze, Analia J. EOP/OMB" (b) (6), "Rodriguez, Drew J. EOP/OMB" <(b) (6), "Croce, Joseph A. EOP/NCD" (b) (6), "Stupak, Philip M. EOP/NCD" (b) (6), CSD Front Office Scheduling <(b) (6), "Presman, Dylan T. EOP/NCD" <(b) (6), "RUSCHMAN, ALEXANDRIA" <(b) (6), "Sardo, Valerie (CTR)" (b) (6), "Smith, Jazmine (CTR)" (b) (6), "Dasher, Grant" <(b) (6), "Lee, Michaela A. EOP/NCD" (b) (6), "Jang, Yejin EOP/OMB" <(b) (6)

Date: Fri, 10 Feb 2023 09:00:49 -0500

Attachments: 26 January 2023_Meeting SOC_OMB-ONCD-CISA Monthly.pdf (193.29 kB)

Hi All,

My apologies for the delay in sending the meeting summary of conclusions. Please find the document attached. We'll look to scheduling the next monthly in the end of February/early March.

V/r,
-Lisa N. Barr

-----Original Appointment-----
From: CSD Executive Assistant Director Scheduler
<(b) (6)
Sent: Friday, January 13, 2023 9:53 AM
To: CSD Executive Assistant Director Scheduler; Dudley, Drenan E. EOP/NCD; Goldstein, Eric (He/Him); Hartman, Matthew (He/Him); Duffy, Michael; Herckis, Mitch D. EOP/OMB; Barr, Lisa N. EOP/NCD; Higgins, Neal L. EOP/NCD; DeRusha, Chris J. EOP/OMB; Mill, Eric R. EOP/OMB; Beckel, Sarah; Romans, Clayton; Roebuck, Jermaine (He/Him); Gross, Martin; Yuhasz, Amy; Conley, Alyson (She/Her); Hartsook, Shelly; Mergen, Margaret C. EOP/OMB; Abrams, Andrew D. EOP/OMB; Butera, Christopher (He/Him); Polk, Nick J. EOP/OMB; Muniz Rodriguez, Christian A. EOP/NCD; Radesky, Sandra (She/Her); Thompson, Robert; Gazlay, Jay (He/Him); LYUBLANOVITS, SHONDREA; Shaw, Robert; Bokan, Branko; Isaac, Kim; Bowen, Ethan; Petrianni, Peter; Cohen, Natasha
Cc: Olamide, Simisola (CTR); Mireles-Beuze, Analia J. EOP/OMB; Rodriguez, Drew J. EOP/OMB; Croce, Joseph A. EOP/NCD; Stupak, Philip M. EOP/NCD; CSD Front Office Scheduling; Presman, Dylan T. EOP/NCD; RUSCHMAN, ALEXANDRIA; Sardo, Valerie (CTR); Smith, Jazmine (CTR); Dasher, Grant; Lee, Michaela A. EOP/NCD; Jang, Yejin EOP/OMB
Subject: CISA/ONCD/OMB Monthly Sync
When: Thursday, January 26, 2023 11:00 AM-12:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

DO NOT FORWARD OR COPY THIS INVITATION
If there are any questions, please contact (b) (6)

Attendees:

- Eric Goldstein, CISA
- Matt Hartman, CISA
- Sandy Radesky, CISA
- Jay Gazlay, CISA
- Mike Duffy, CISA
- Shelly Hartsook, CISA
- Chris Butera, CISA
- Sarah Beckel, CISA
- Clayton Romans, CISA
- Jermaine Roebuck, CISA
- Bobby Thompson, CISA
- Martin Gross, CISA
- Amy Yuhasz, CISA
- Alyson Conley, CISA
- Shondrea Lyublanovits, CISA
- Robert Shaw, CISA
- Branko Bokan, CISA
- Kim Isaac, CISA
- Peter Petrianni, CISA
- Ethan Bowen, CISA
- Natasha Cohen, CISA
- Chris J. DeRusha, EOP/OMB
- Mitchel D. Herckis, EOP/OMB

- Eric Mill, EOP/OMB Senior Advisor
- Lisa N. Barr, EOP/NCD
- Neal L. Higgins, EOP/NCD
- Maggie Mergen, OMB
- Andrew Abrams, EOP/OMB
- Nick Polk, EOP/OMB
- Drenan Dudley, EOP/NCD
- Christian Muniz, EOP/NCD

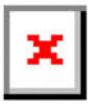
Objective: Monthly recurring meeting with CISA, ONCD, and OMB leadership teams.

Briefing Materials: N/A

Microsoft Teams meeting

Join on your computer, mobile app or room device
Click here to join the meeting

Meeting ID: 215 200 166 196
Passcode: SuKvgA
Download Teams | Join on the web



* * * * * U.S. Department of Homeland Security * * * * *

Learn More | Meeting options

Monthly Meeting: OMB, ONCD and CISA
Summary of Conclusions

DATE: Thursday, January 26, 2023
TIME: 11:00am – Noon ET
LOCATION: MS Teams
ATTENDEES: OMB, ONCD, CISA

BOTTOM LINE UP FRONT (BLUF)

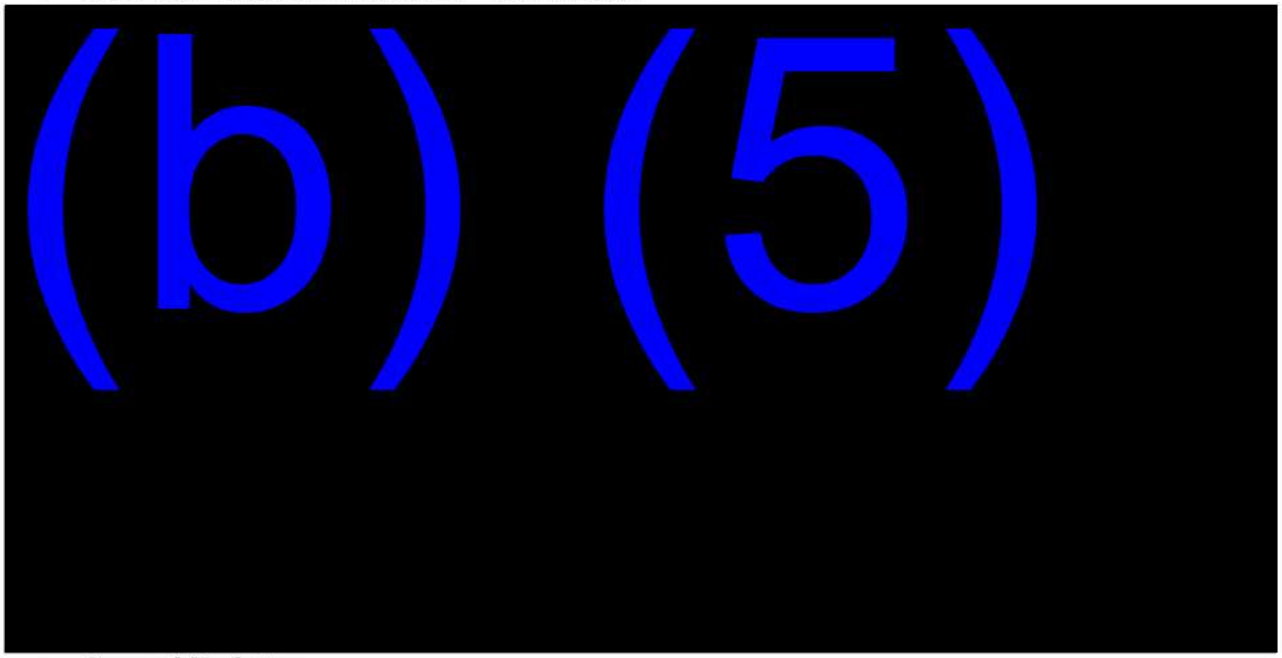
Monthly sync to coordinate shared initiative(s) and elevate decisions, risks, and issues for OMB, ONCD, and CISA leadership

OBJECTIVES/DESIRED OUTCOME OF MEETING:

- Agreement on priorities and upcoming activities
- Shared knowledge and visibility of initiatives
- Cohesive leadership decision-making

DISCUSSION POINTS:

- Priority/Hot Topics – 10 Minutes
  -
- Areas for Cross-collaboration – 20 Minutes



- General Updates:
  - National Cybersecurity Strategy Rollout/update – Brief update/overview provided on the current state of NCD.

  - TikTok prohibition and implications across government – Brief update provided on the status of the TikTock memo.
  - WH Summit Spring 2023– Beyond PIV/Identity management – Brief update provided on an upcoming/planning WH summit in May 2023 focusing on moving beyond PIV and working with industry on alternate phishing resistant MFA mechanisms.
- Key Decision Points, Risks and Issues – N/A
- Walk-through Cross-Coordination Tracker – N/A
- Close out

ACTION ITEMS

CISA to convene small group to work on developing a plan to address logging challenges with M-21-31 [Action: CISA to report status and updates at next Monthly.]

Next Monthly Meeting: February 2023

[MSC] Intel Update - 14 February 2023

From: "Manteghi, Amir D. EOP/NCD" (b) (6)
To: "Walden, Kemba E. EOP/NCD" <(b) (6) >, "Leiserson, Nick J. EOP/NCD" <(b) (6) >, "Suarez, Amanda R. EOP/NCD" <(b) (6) >
Cc: "Ring, Haley A. EOP/NCD" <(b) (6) >, "Chang, Caroline EOP/NCD" (b) (6) >, "Stupak, Philip M. EOP/NCD" <(b) (6) >, "Higgins, Neal L. EOP/NCD" (b) (6) >, "Todoroff, Joel D. EOP/NCD" (b) (6) , "Krejsa, Harry H. EOP/NCD" <(b) (6) >
Date: Tue, 14 Feb 2023 01:30:21 -0500
Attachments: 1. ONCD Intelligence_Update_MSC_02.14.23.pdf (371.48 kB); 2. REUTERS Chinese mobile masts loom over the Munich Security Conference.pdf (223.29 kB); 3. EFIS_ENG-report_2023_reduced.pdf (5.81 MB); 4. FA_commercial_spyware.pdf (1.47 MB)

Kemba, Nick, Amanda,

Starting a rhythm to provide unclassified "intelligence and analysis" updates that should sustain you in various MSC conversations. As you know, many of your counterparts will have dedicated intel staff with them to perform this function; driving morning updates via feedback from evening team debriefs. However, Joel and I will do our best to flag appropriate material remotely to hopefully ensure the team's success. And, since the team will not have secure comms, unclass will be the best we can do this time around, which I think, for the most part, is sufficient.

Attached is the first version, with additional referenced attachments for deeper reading, as time permits, given your first day is a travel day with more time to read. Updates should land in your queues around 7AM, (late evenings EST) FWIW. If you have additional information needs, as we move forward, send them over.

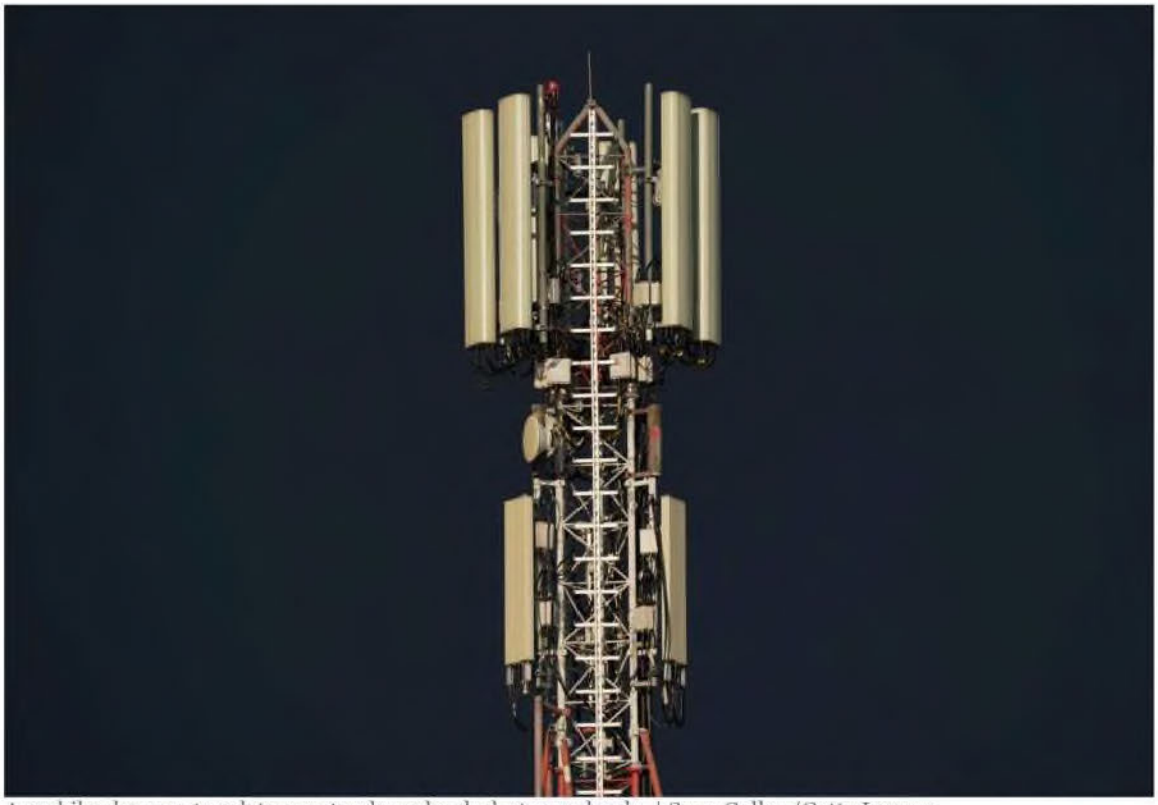
Safe travels,
Amir + Joel

Amir Manteghi
Director for Intelligence Support
Office of the National Cyber Director
(b) (6)
(b) (6)

POLITICOPRO

Chinese mobile masts loom over the Munich Security Conference

BY LOUIS WESTENDARP, ANTOANETA ROUSSI, LAURENS CERULUS
02/13/2023 04:39 PM EST



A mobile phone network tower stands under dark storm clouds. | Sean Gallup/Getty Images

MUNICH — As the world's security elite gathers in Munich this week, they'll be connecting their mobile phones to Chinese telecoms equipment surrounding the venue.

Heads of state, security chiefs, spooks and intelligence officials head to Germany on Friday for their blue-riband annual gathering, the Munich Security Conference. On the event's VIP list are U.S. Vice President Kamala Harris, German President Olaf

NCD008FY23023_000000389

Scholz, French President Emmanuel Macron and hundreds more heads of state and government, ministers and foreign dignitaries.

The gathering takes place at the five-star Hotel Bayerischer Hof. From its ice-themed Polar Bar on the hotel's rooftop, you can overlook the city's skyline, spotting multiple telecommunications antennas poking between church steeples. Some of these antennas, within 300 meters of the hotel, are equipped with hardware supplied by controversial Chinese telecoms giant Huawei, POLITICO has learnt through visual confirmation, talks with several equipment experts and information from industry insiders with knowledge of the area's networks.

One mast, on top of the Hotel Bayerischer Hof building itself, is also potentially equipped with Huawei gear, talks with two industry insiders suggested.

The question of whether to allow Chinese 5G suppliers into Western countries in past years became a bone of contention between Berlin on the one hand and Washington and like-minded partners on the other. This week's gathering also comes as the U.S. continues to call out Germany's economic reliance on Beijing, with a new report showing the German trade deficit with China exploded in 2022, and amid sky-high tensions between Washington and Beijing over surveillance balloons hovering over the U.S., Canada and elsewhere.

"The dependence on Huawei components in our 5G network continues to pose an incalculable security risk," said Maximilian Funke-Kaiser, liberal member of the German Bundestag and digital policy speaker for the government party Free Democratic Party (FDP).

"The use of Huawei technology in the mobile network here runs counter to Germany's security policy goals," Funke-Kaiser said, calling the vendor's involvement in German 4G and 5G "a mistake in view of the Chinese company's closeness to the state."

Huawei has consistently denied posing a security risk to European countries.

Delving into data

Despite extensive reporting, POLITICO was unable to gather on-the-record confirmation of which vendor's telecoms equipment was used for which masts. Operators and vendors refused to disclose the information, citing contractual obligations, and local authorities said they didn't have the information available.

The security risks associated with Huawei equipment also vary, and differ even among close allies in the West. Some capitals argue the real risk of Chinese telecoms equipment is the overreliance on a Chinese firm in an unstable geopolitical situation — much like Europe relied on Russian gas for its energy needs.

But others argue that the risk runs deeper and that China could use Huawei's access to equipment and data in European mobile networks — especially in areas of critical importance and high sensitivity — to put the West's security at risk. Huawei has been implicated in a number of high-profile espionage cases, including at the African Union Headquarters.

When asked about Huawei's presence in Munich, Mike Gallagher, a Republican and Chairman of the U.S. House select committee on China, said POLITICO's findings were "troubling" and "should concern every individual attending the conference."

The chair of the U.S. Senate intelligence committee, Mark Warner, a Democrat who's attending the conference, said it was "a timely reminder that we must continue to work with like-minded allies to promote secure and competitively priced alternatives to Huawei equipment."

U.S. Senate intelligence committee Vice Chair Marco Rubio (Republican, Florida) said U.S. diplomats "should be aware of the risks and take necessary precautions."

Munich networking

From a 2007 speech by Russia's Vladimir Putin to U.S. President Joe Biden's virtual address at the start of his mandate in February 2021, the conference strives to set the global diplomatic and international relations agenda. Its organizers see it as an open space for debating geopolitics and world affairs, with attendees ranging from across the world and an advisory board where Chinese state officials sit alongside Western diplomats and titans of industry.

The conference's guest list reveals something else too: The gathering is seen as critical by U.S. government officials. This year, the U.S. is sending its largest delegation yet, with Harris flanked by dozens of government officials, security chiefs and congresspeople, including Democrat leader Chuck Schumer, Republican leader Mitch McConnell and others.

For these U.S. attendees — and the Western partners that see eye to eye with the U.S. position on China's telecoms giant Huawei — the networks around the premises prove troublesome.

An online map on the website of Germany's telecoms agency, the Bundesnetzagentur, shows 13 locations for masts and antennas surrounding the Hotel Bayerischer Hof. The agency also provides information about which of the country's three main operators — Deutsche Telekom, Vodafone and Telefónica — use which locations.

POLITICO shared photos of seven masts near the hotel with four experts specialized in telecoms radio access network (RAN) equipment. These experts established that at least two were equipped with gear of Chinese telecoms giant Huawei.

If a network operator has one mast equipped with Huawei in Munich, it likely equips all masts in the area with the same vendor, two industry insiders said. Operators usually use one provider for larger areas. This means at least one other location is also likely equipped with Huawei gear, the insiders said. Three other locations, including the mast on the roof of the conference venue, are used by an operator using Huawei equipment but those locations are part of infrastructure that is shared by several operators, meaning there's a chance these are equipped with Huawei gear but it's unconfirmed.

The findings are in line with recent reports on Germany's telecoms infrastructure.

Europe's largest economy is a stronghold for Huawei in the West. A report by boutique telecoms intelligence firm Strand Consult estimated that Germany relies on Chinese technology for 59 percent of its ongoing 5G network deployment. The country already had a massive reliance on Chinese equipment in its 4G network, where Strand estimated Huawei accounts for 57 percent.

"If you look at the percentage of Chinese equipment in Germany, you could say it is the most unsafe country in Europe," said John Strand, founder of Strand Consult. "Welcome to the Munich Security Conference: We can't guarantee your security," he quipped.

Black hole of telecoms intelligence

Establishing with certainty just how many of the 13 masts are equipped with Chinese telecoms gear is extremely difficult. Both German operators and their vendors have a policy to not communicate what equipment they're using in which locations, citing contractual obligations on confidentiality.

Deutsche Telekom and Vodafone confirmed that they use Huawei in their German antenna networks. Telefónica said they use "a mix of European and international network suppliers" in Germany. Yet, all declined to comment on whether they use Huawei in Munich.

Ericsson, Nokia and Huawei all declined to comment on whether they were providing gear in the greater Munich area, referring questions to the local operators.

Government regulators, too, divulge no details of which suppliers provide gear for certain locations. The Federal Network Agency and the Federal Office for Information Security admitted they don't know which equipment is fitted to which mast; both referred to the interior ministry for answers. The interior ministry said it "does not usually know which critical components are installed on which radio mast in detail."

The Hotel Bayerischer Hof forwarded questions about mobile infrastructure on its roof to the security conference's organizers.

The Munich Security Conference itself said in a statement: "As a matter of principle, we do not comment on the exact details of the infrastructure used for the main conference in Munich. We are in close contact with all relevant authorities in order to secure the conference venue, the participants and the digital space accordingly."

The Federal Office for Information Security (BSI) does provide its own security networks for official events, but the Munich Security Conference is "outside the responsibility of the BSI," the BSI said in an email.

Germany's telecoms ambiguity

Through its 5G equipment it is feasible for Huawei to spy on users of a network or to disrupt communications as the very design of 5G makes it harder to monitor security, the head of the U.K.'s intelligence service MI6, Alex Younger, said to an audience in his second public speech.

But John Lee, director of the consultancy East-West Futures and an expert on Chinese digital policy, said it's "not a clear cut technical case" as to whether Huawei equipment in current telecoms networks represents a material security risk.

"Some non-Western countries are proceeding to upgrade their telecoms infrastructure with Huawei as a key partner," Lee said. "This is still mainly a political issue of how much suspicion is placed on the ambitions of the Chinese state and its relationship with Chinese companies."

In an effort to coordinate a common approach to vendors, the EU developed "5G security toolbox" guidelines in 2019 and 2020 to mitigate security risks in networks. Some major European countries, including France, have imposed hard restrictions for their operators, including by limiting the use of "high-risk vendors" — a term widely understood across Europe to be Chinese vendors Huawei and ZTE — in certain strategic geographic areas.

In Germany, however, policymakers took years to agree on their framework for 5G security. In April 2021 — more than a year after the EU's joint plan came out — it passed measures that allowed the government to intervene on operators' contracts with Chinese vendors.

But those interventions haven't barred the use of Huawei in certain geographical areas yet.

And the interior ministry — which has veto power to ban or recall certain components if they see them as an "impairment of public order or safety" — hasn't intervened much either, a ministry spokesperson said via email.

Up till now, the spokesperson said, specific orders to cut Huawei from German networks "have not been issued."

Alex Ward, Maggie Miller and Tristan Fiedler contributed reporting.

INTERNATIONAL SECURITY AND ESTONIA 2023



Estonian Foreign Intelligence Service

NCD008FY23023_000000388

INTERNATIONAL SECURITY AND ESTONIA 2023

Estonian Foreign Intelligence Service

NCD008FY23023_000000388

FOREWORD



DEAR READER,

You are holding the eighth edition of the Foreign Intelligence Service's annual report, the first I have the honour to present as Director General. At a time when Europe is witnessing its biggest war since 1945, the thirst for intelligence services' situation reports and analyses has grown. We seek to fulfil our role to the best of our ability.

In last year's report, we wrote that Russia would create the conditions and capabilities necessary to launch a large-scale military offensive against Ukraine in the second half of February 2022. Unfortunately, that is what happened.

Russia has so far failed in its war of aggression. It attacked Ukraine with a plan for a quick coup based on absurd assumptions and a manipulated intelligence picture. In the first months of the war, the Ukrainians destroyed a significant part of the best units of the Russian army, which, as the war drags on, has led to Russia's critical need for mobilised troops, private military companies and arms from pariah states. The war strangles the Russian economy and raises the temperature in otherwise apolitical Russian society. The Russian elite is increasingly discussing whether "the First Person has gone mad", but most of them lack the courage to take real steps towards change. Russia's stubbornly imperialist stance towards its neighbours persists, and Russians' fear of mobilisation surpasses their sense of responsibility for the genocide committed by their compatriots.

Despite setbacks and risks, Vladimir Putin's goal in Ukraine has not changed by early 2023. For now, there is still enough fuel to keep the war machine going – Russia will not run out of cannon fodder, Soviet-era armaments or propaganda-induced imperialism any time soon. However, a quality leap in Russia's war-fighting capability is very unlikely. Putin is playing for time, believing that Ukraine and the West will wear out before Russia. Putin thinks he can "bomb" Ukraine to the negotiating table.

Internally, Russia has become Soviet Union 2.0, drawing inspiration from Stalinist repression, Khrushchevian sloganeering and Brezhnevian stagnation. Paradoxically, in Russia today, Putin's regime is simultaneously the strongest and the weakest it has ever been. But there seems to be no new Gorbachev, not to mention Yeltsin, on the horizon. The democratic world should not harbour illusions that post-Putin Russia will embrace democratic values any time soon.

This year's report also discusses the course change in Russian foreign policy. Russian diplomats, led by Foreign Minister Sergei Lavrov, were caught off guard by the war in Ukraine. Realising that it lacks influence on strategic issues has led the Russian foreign ministry's morale to decline. Russia has given up on the West for the foreseeable future and is seeking new friends, mainly in Africa and Asia.

Once again, we will also look at China. Under the leadership of Xi Jinping, who started his third term and secured absolute power, China is moving towards deepening authoritarianism and confrontation with the West. Russia plays an important role in China's global ambitions, and the two countries agree on many points. Therefore, it would be a mistake to take Xi's restrained support for Putin's war in Ukraine as a sign that China is distancing itself from Russia.

The Foreign Intelligence Service celebrated its 30th anniversary a few months ago. With our domestic and international partners, we continue to work to ensure that the Estonian leadership and our allies have the best information on the security situation and sufficient advance warning. And to ensure that Ukraine wins.

Bravely onward and *Sláva Ukrayíni*!

Kaupo Rosin
Director General, Estonian Foreign Intelligence Service
31 January 2023

TABLE OF CONTENTS

1. CHAPTER: RUSSIAN ARMED FORCES AND THE WAR IN UKRAINE 9

- Russia's War Against Ukraine 10
- Russian Armed Forces Near The Estonian Border 12
- Russia Continues To Look For A Weak Link In Ukrainian Cyberspace 14
- Belarus As A Foothold In The Ukrainian Conflict 18
- Russian Administration In The Occupied Territories Of Ukraine 21

2. CHAPTER: RUSSIAN FOREIGN POLICY 25

- 'Regrouping' Of Russian Foreign Policy 26
- A Paper Tiger In The Caucasus 30
- Russia's African Policy 32

3. CHAPTER: RUSSIAN DOMESTIC POLITICS AND ECONOMY 37

- Russia's Domestic Political Situation 38
- The Russian Economy 42

4. CHAPTER: RUSSIAN SPECIAL SERVICES 47

- Covers Used By Russian Intelligence Services 48
- The Russian Special Services' Support To President Putin 52

5. CHAPTER: RUSSIAN INFLUENCE 55

- The Candle Of The 'Russian World' Is Burning Out 56

6. CHAPTER: CHINA 61

- China's Global Embrace 62
- China's Calculations On Attacking Taiwan 64
- Chinese-Russian Relations In The Context Of The War In Ukraine 66

EXECUTIVE SUMMARY

1. The Ukrainians' will to defend, the capabilities of their Armed Forces, and Western unity in supporting Ukraine surprised the Kremlin. Despite this, Russia's strategic goal remains the same: subjugating Ukraine and changing the European security architecture. *Read more in chapters 1.1, 2.1*

2. Russia believes that time is on its side. To keep the war machine going, Russia is ready raise the stakes. Russia seems to believe it can "bomb" Ukraine to the negotiating table. *Read more in chapter 1.1*

3. Russia's belligerence has significantly increased the security risks for Estonia, and the large-scale exercise Zapad 23 may further strain the situation in the Baltic Sea region. Russia still has enough strength to exert credible military pressure in our region. *Read more in chapter 1.2*

4. Russia supports its military efforts in Ukraine by using cyber tools against Ukraine and the countries that support it. Its activities in cyberspace have not yielded the results Russia had hoped for, but we must remain vigilant. *Read more in chapter 1.3*

5. The Russian special services officers hide behind various "covers". A tried-and-tested cover organisation used abroad is the Russian Orthodox Church, which the Kremlin also operates as an instrument of influence against Ukraine and the West. *Read more in chapters 4, 5*

6. Belarus has provided logistical and material support to Russia in the war against Ukraine, but the Belarusian Armed Forces have not yet intervened in the military operations in Ukraine and do not wish to do so in the future. *Read more in chapter 1.4*

7. Russia is moving towards a total dictatorship. The prospects for the current regime collapsing and the country democratising are slim despite the problems caused by the war and Western sanctions. On the contrary, an even more radical faction is rising to the fore in Russia's ruling elite. *Read more in chapter 3.1*

8. In foreign policy, Russia has its stakes on creating a geopolitical coalition of authoritarian regimes opposed to the West who share a mistrust of Western policies and values. Diplomatic resources are being diverted from the West to other regions. *Read more in chapter 2.1*

9. Russia's military credibility in former Soviet territories has weakened because Russia has failed to provide the security guarantees promised within the CSTO framework, and its Armed Forces have been unsuccessful in Ukraine. In Africa, however, Russia sees its best opportunities precisely in the field of security. *Read more in chapters 2.2, 2.3*

10. Under Xi Jinping, China is moving towards deepening authoritarianism and no longer hides its ambition to become a global superpower. China's efforts to build a community of like-minded countries opposed to the West under the banner of the Global Security Initiative – which would also include Russia – undermines Estonia's security. *Read more in chapter 6*

CHAPTER 1

RUSSIAN ARMED FORCES AND THE WAR IN UKRAINE

8

NCD008FY23023_000000388

RUSSIA'S WAR AGAINST UKRAINE

Subjugating Ukraine and reshaping European security architecture remains Russia's strategic objective.

Russia believes time is on its side in the war as Ukraine and its partners are less prepared to sustain a drawn-out conflict.

Russia plans to mobilise additional resources to support its military action, continuing the war into 2023.

The invasion of Ukraine, which began in the early hours of 24 February 2022, is a continuation of Russia's almost nine-year-old aggression against Ukraine. Russia's strategic objective – to subjugate Ukraine and thereby decisively reshape European security architecture – has not changed over time.

Russia is ready to continue raising the stakes in Ukraine through further mobilisation or expanding terror tactics against the civilian population.

As with the covert invasion of 2014, Russia's plan to subjugate Ukraine in early 2022 was based on false assumptions and biased intelligence: Ukrainians' will to defend, the combat capabilities of the Armed Forces and the widespread Western support for Kyiv were completely unexpected for Russia. A lack of alternative courses of action also aggravated the situation for the Russian Armed Forces. This was probably due to unusually rigid operational security requirements, which meant the headquarters of some of the units of the Russian Armed Forces deployed close to the Ukrainian border were unaware of the imminent invasion and did not prepare appropriate plans for combat support and combat service support for the invasion. The Russian Armed Forces' plan to occupy Kyiv, overthrow the Ukrainian government and take control of the territory proved unfeasible, at least within the expected timeframe and with the units available.

Since realising the impracticability of the initial course of action, Russia has decisively adjusted its plans twice to avoid defeat and try to regain the initiative: first, in March and April 2022, by withdrawing from northern Ukraine and focusing on invading eastern and southern Ukraine, and second, in September, when Russia announced mobilisation. Both actions exemplify Russia's readiness to escalate and, if necessary, change its plans. Russia is ready to continue raising the stakes in Ukraine through further mobilisation or expanding terror tactics against the civilian population. Whilst the use of tactical nuclear weapons in Ukraine is unlikely due to international opposition and low military effectiveness, Russia continues to keep the "nuclear card" on the table as an instrument of anti-Western leverage to instil fear of war and to dissuade Western nations from helping Ukraine.



Russia was much more ambitious in 2013-14 than the Kremlin officially admitted. According to EFIS' information, Russia planned for the occupation of 11 Ukrainian regions.

The continued readiness of Western countries to support Ukraine is, therefore, crucial to raise the cost of continuing the war for Russia.

Russia believes that time is on its side in the war in Ukraine – the Kremlin's mobilised reserves are being trained, lost military equipment is being replaced by weaponry stored in the mobilisation depots, and, at the same time, Russia is systematically destroying Ukraine's critical civilian infrastructure, hoping to break the Ukrainians' will to defend. Russia probably plans to deploy its mobilised reserves at the end of their training in the first half of 2023 in a new offensive. Despite the losses suffered and problems in producing war materials and new weapon systems, Russia intends to continue its military action against Ukraine in 2023. To this end, the Kremlin plans to mobilise additional human and industrial resources to support the military action, looking for opportunities to source arms and ammunition from other countries, such as Iran, Belarus and North Korea.

Russia's strategic objectives remain unchanged despite military defeats; the subjugation of Ukraine, the erosion of Western unity and the transformation of European security remain at the core of Russia's geopolitical ambitions. The Russia-Ukraine war will continue in 2023, given that Russia has so far lacked sincere interest in peace talks, as these would not ensure the fulfilment of the Kremlin's strategic objectives. While Putin still seems to believe that time will play in Russia's favour and he will be able to "bomb" Ukraine to the negotiating table, reality will dawn on the Kremlin sooner or later. The continued readiness of Western countries to support Ukraine is, therefore, crucial to raise the cost of continuing the war for Russia.

RUSSIAN ARMED FORCES NEAR THE ESTONIAN BORDER

A military attack against Estonia is unlikely in 2023 because Russia's military capabilities are engaged in Ukraine. However, in the mid-to-long term, Russia's belligerence and foreign policy ambitions have significantly increased the security risks for Estonia.

Mobilisation and large-scale exercises planned by Russia could further strain the security situation in the Baltic Sea region in 2023.

From the Baltic states' perspective, Russia still has enough military capability to exert credible military pressure in our region. The capabilities of the Russian Armed Forces in the immediate vicinity of the Estonian border can be quantitatively reconstituted in up to four years.

The only existential threat to the security of our region, including Estonia's sovereignty, stems from Russia. A military attack against Estonia is unlikely in 2023, as the Russian Armed Forces units based near the Estonian border are engaged in hostilities in Ukraine. At the same time, Russia's foreign policy ambitions driven by the Kremlin's belligerence and imperialism have significantly increased the security threat. If Russia were diplomatically or militarily successful in Ukraine, it would increase the risk of the Kremlin's political and military pressure on the Baltic states in the mid-2020s.

If Russia were diplomatically or militarily successful in Ukraine, it would increase the risk of the Kremlin's political and military pressure on the Baltic states in the mid-2020s.

From the first day of the war, the 76th Guards Air Assault Division and elements of the 6th Army of the Russian Armed Forces, which are responsible for covering the Estonian operational direction, have been involved in battles in Ukraine and suffered heavy losses. The mobilisation launched in September 2022 has also affected Pskov and Leningrad oblasts, with reservists mobilised in both regions and sent to combat units in Ukraine to compensate for losses. The training areas and training centres in both oblasts have also been used to train new reservist units. Although Russia's mobilisation reserves have enough equipment to form new units, finding competent personnel for the units' headquarters may be unrealistic. Many Russian Armed Forces instructors have been transferred away from the training centres to join combat units in Ukraine, which has led to a declined level of training and reduced cohesion of the mobilised units.

Due to heavy losses, the Russian Armed Forces face a significant shortage of junior and senior officers. The shortage of junior officers has been compensated for by accelerating the graduation process in military schools, which has a negative impact on the officers' qualifications. However, there are no quick fixes to make up for the shortage of senior officers.

The Russian Armed Forces plan to carry out the Zapad 2023 manoeuvres this year. The term "manoeuvre" is Russian military jargon typically used to describe a large-scale strategic exercise, that takes place in more than one strategic direction. In Russia, the Armed Forces' annual training cycle culminates with a joint strategic exercise, which rotates from year to year between the four military districts (e.g., Kavkaz 2020, Zapad 2021, and Vostok 2022), but these do not always qualify as manoeuvres in terms of scale. Zapad 2023 is not a regular part of the rotation of strategic exercises, which should have seen Tsentr 2023 taking place instead. A departure from the expected training cycle with a large-scale joint strategic exercise in the western strategic direction at the same time as the military action in Ukraine can be seen as a deterrent and threat to the West and as an incitement to patriotism among the Russian population.

From Estonia's point of view, it is important to demonstrate NATO's military readiness to dissuade Russia's temptation to test the Alliance's security guarantees.

Russia considers the Baltic states to be the most vulnerable part of NATO, which would make them a focus of military pressure in the event of a NATO-Russia conflict. Therefore, Russia is highly likely to give priority to reconstituting its military capabilities, weakened in the war in Ukraine, in the immediate vicinity of the Estonian border. The quantitative reconstitution of these units' capabilities will take up to four years. From the Baltic states' perspective, Russia still has enough strength to exert credible military pressure in our region.

From Estonia's point of view, it is important to demonstrate NATO's military readiness to dissuade Russia's temptation to test the Alliance's security guarantees. The probability of a military conflict between NATO and Russia would increase if Russia were to achieve its strategic objectives in Ukraine. Therefore, Ukraine's victory in the war against Russia would also improve regional security.



Russian Armed Forces destroy critical infrastructure and use terror tactics against the civilian population.

Source: Roman Pilipey / EPA

NCD008FY23023_000000388

RUSSIA CONTINUES TO LOOK FOR A WEAK LINK IN UKRAINIAN CYBERSPACE

Russia uses cyberattacks to support its general goals in Ukraine: to break Ukrainian resistance, undermine the government's image and disrupt the functioning of the state. Cyber espionage is likely the biggest threat stemming from cyberspace.

Russia underestimated the resilience of Ukraine's cyberspace and the help it receives from Western countries and cybersecurity companies.

Threats posted on social media and cyberattacks continue as part of the influence operations against countries that actively support Ukraine, including Estonia.

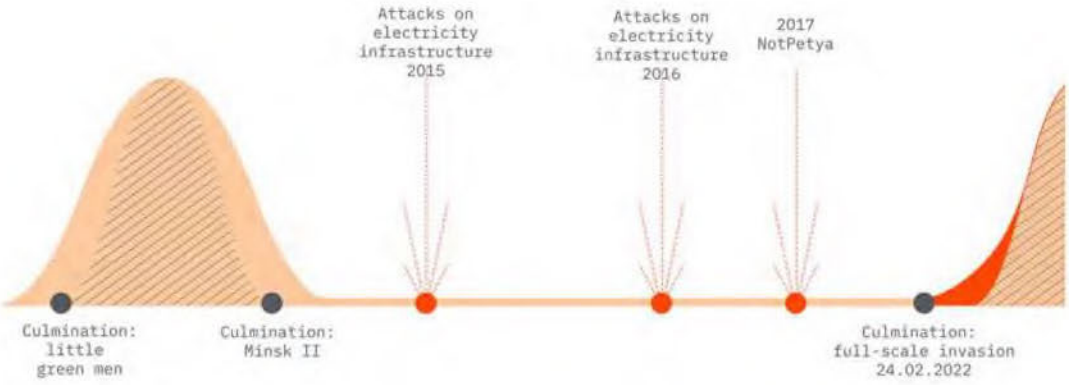
At least since the start of the Russo-Ukrainian war in 2014, Ukraine has been a constant target of cyberattacks by Russian special services.[1] Attacks intensified immediately before kinetic warfare began and continued throughout the active phase of the war. Russia mainly organised cyberattacks as part of influence operations, such as denial-of-service and defacement attacks and data leaks. One of the goals of these activities is to prevent the Ukrainian government from sharing information with its citizens, to cause fear and distrust in the state's leadership, to weaken society's resistance and to create information noise that makes it difficult to distinguish reality from disinformation. After the most active phase of kinetic warfare, Russia tried to keep the Ukrainian state weak and organised cyberattacks to disrupt critical services.[2] Low-intensity cyberattacks, mainly for intelligence purposes, were conducted until Russia again stepped up its aggressive rhetoric towards Ukraine. In January and February 2022, Russia's cyberattacks against Ukraine seemed to be aimed at supporting its general goals: to break the resistance of the Ukrainian population and create an impression of Russia's vast superiority, the hopelessness of the situation for Ukraine and the weakness of the Ukrainian state.

> From 13 to 14 January 2022, cyberattackers broke into the websites of Ukrainian state institutions and made these inaccessible to the public. During the same period, cyberattackers spread the WhisperKill/WhisperGate malware in Ukrainian computer networks.[3]

1 At least since 2014, the FSB's 18th Centre has been directing cyberattacks against Ukraine, including stealing information, https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys -kiberatak-na-derzhavni-orhany-ukrainy.

2 In December 2015 and 2016, the GRU carried out cyberattacks on Ukraine's energy sector, which led to several-hour power outages in Western Ukraine. In 2017, the GRU organised the NotPetya cyber operation to make Ukrainian government agencies' data unusable. https://www.wired.com/story/sandworm-kremlin-most-dangerous-hackers

3 https://cert.gov.ua/article/18101; https://ssu.gov.ua/en/novyny/sbu-rozsliduie-prychetnist-rosiiskykh-spetssluzhb-do-sohodnishnoi-kiberataky-na-orhany-derzhavnoi-vlady-ukrainy; https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion; 27 April 2022, Microsoft, Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.



From 15 to 16 February 2022, denial-of-service attacks took place against the websites of Ukrainian state institutions and banks.[4]

A few hours before the reactivation of kinetic warfare, cyberattacks against Ukraine suddenly increased even more.

On 23 February 2022, denial-of-service attacks took place against the websites of Ukrainian state institutions and banks.

From 23 to 25 February 2022, cyberattackers installed several types of malware in Ukrainian information systems, which can disrupt computer use or make data on the computer inaccessible. For example, on 23 February, the GRU installed the destructive HermeticWiper malware in the information systems of Ukrainian government agencies, the IT sector, and the energy and financial sectors. On 24 February, it conducted a cyberattack on Viasat's subsidiary KA-SAT by installing the AcidRain malware in the latter's information system.[5]

While the West distinguishes between cyberattacks and influence operations, Russia interprets them as a single concept – information confrontation (*информационное противоборство*). This Russian Armed Forces' doctrine consists of three main components: exerting informational, technological and psychological influence on another country, and protecting Russia itself from such influences.

It is possible that specific cyberattacks against energy, water supply or other similar critical infrastructure,[6] which would lead to long-term service interruptions, were not organised early on because Russia expected to achieve its military objectives quicker and wanted to maintain the support of the local population.

4 An overview of Russia's cyberattack activity in Ukraine. 27 April 2022, Microsoft, Special Report: Ukraine.
5 https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-oneurope/
6 An attack on the specific industrial control information systems, which are used for vital services such as energy and water supply, is somewhat different from attacking ordinary information systems. Simply put, these information systems are built differently. The Industroyer2 malware was specially developed to attack industrial control information systems, and the GRU probably used it on 8 April 2022 against the Ukrainian energy sector. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Despite failing to occupy Ukraine in a few days as originally intended, Russia continued its cyberattacks against Ukraine. These were more frequent during certain periods. For example, Ukrainian cyber defenders working with cybersecurity companies repeatedly detected destructive malware over a period of about 30 days from the second half of March. Cyberattacks started to gain momentum again in the autumn.[7] Cyberattacks to obtain information have continued.[8] Cyber espionage is likely the biggest threat stemming from cyberspace. Stolen information can effectively be used as input to Russian special services' operations and influence activities.

> During the war, Russia has used several destructive malware repeatedly. On 11 October 2022, Microsoft detected the CaddyWiper malware in the critical infrastructure of the Mykolaiv and Kyiv regions. The cybersecurity company ESET detected this malware for the first time on 14 March 2022 in the information system of a Ukrainian bank.[9]
>
> On 14 October 2022, Microsoft identified the Prestige ransomware in the information system of Ukrainian and Polish logistics and transport companies.

In 2022, cybersecurity researchers identified at least nine types of destructive malware in Ukrainian cyberspace that have attempted to disrupt services (ENISA Threat Landscape 2022, p. 25; Recorded Future, 2022). Destructive malware makes a computer unusable by corrupting programs or data. Ransomware that encrypts data without the possibility of decrypting, such as Prestige, can be used to the same end. Such an amount of destructive malware has never been observed anywhere in such a short period of time. This shows that Russia is capable of quickly developing new malware.

Russian cyberattacks, like the actions of its armed forces, are likely aimed at wearing down Ukraine's cyber defenders and then finding the weakest link that would help achieve Russia's overall military goal – to wear down Ukraine, damage the international image and credibility of the Ukrainian leadership, reduce aid from allies, and undermine the society's morale. Therefore, a cyberattack need not actually disrupt an information system, as with each attack, investigators have to spend human and time resources to check whether and how extensively the information system has been attacked, how to improve defence, etc.

Russia underestimated the resilience of Ukraine's cyberspace and the help it receives from Western countries and cybersecurity companies. Despite denial-of-service attacks on the websites of state institutions to disrupt the flow of information, among other things, the Ukrainian government has found alternative ways of communication, for example, using social media. Using Starlink devices also plays an important role in maintaining civilian and military communications. Cybersecurity companies have been helping Ukraine defend its cyberspace since 2014. Aid intensified during the full-scale Russian invasion and, with allied support, was likely instrumental in ensuring the resilience of Ukraine's cyberspace. Russia's influence operations in cyberspace have not had the expected effect. Ukrainian society remains united and trusts its government despite threats posted on social media and data leaks.

7 On detected cyberattacks, see e.g. https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/
8 https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/
9 https://twitter.com/ESETresearch/status/1503436420886712321

Russian cyberattacks go beyond the territory of Ukraine. Pro-Kremlin cyberattackers threaten the cyberspace of countries that support Ukraine, including Estonia, Latvia, Lithuania and Poland. In the active phase of kinetic warfare, they have attempted to intimidate societies with threats on social media, denial-of-service attacks and data leaks. Their activities support Russian special services' influence operations.

> From 16 to 17 August 2022, denial-of-service attacks took place on the information systems of Estonian companies and state institutions.[10] Pro-Russian hacktivists took responsibility for these cyberattacks and claimed to have attacked 207 targets in Estonia.[11] In fact, they just copied a list of services where the Smart-ID app can be used, and actual attacks were not carried out against all these targets.

Russia uses cyberattacks to support its strategic objectives (e.g., causing fear and weakening society's resistance to the aggressor, disrupting the functioning of the state, and creating information noise to make it difficult to distinguish reality from disinformation). The Russo-Ukrainian war confirms that cybersecurity measures[12] make it possible to withstand cyber espionage, cyber sabotage and influence operations.

Instrument of Attack	Purpose	Protective Measure
defacement attacks	• intimidation/threatening • creating confusion • disrupting information flow	Website software update. When outsourcing a website, make sure the provider diligently implements cybersecurity measures. If defaced, use alternative information channels if possible, such as social media. Main targets: media, state institutions (mediators of crisis information), website providers
denial-of-service attacks	• disrupting information flow • intimidation	Protection against denial-of-service attacks (see RIA suggestions)[13]
social media posts	• intimidation/threatening	Check the information against reliable sources and be critical of sources. See advice on the conduct of information warfare from the website kriis.ee
data leaks	• damage to reputation (reduce help from allies and intelligence sharing)	Think carefully about what information you share and with whom. Make sure your shared information is kept secure, and the recipient keeps the shared information in an environment where cybersecurity best practices are implemented.
data encrypting malware	• disrupting the functioning of the state • intimidation	Back up data properly
destructive malware	• disrupting the functioning of the state • intimidation	Keep your software updated. Implement cybersecurity best practices. Back up data properly
cyber intelligence (phishing, brute force attacks, exploitation of security vulnerabilities)	• information gathering • leaking stolen information out of context, combined with fabricated information	Keep your software updated. Implement cybersecurity best practices. Get cyber hygiene training

10 https://www.ria.ee/en/news/ddos-attacks-16th-and-17th-august-targeted-around-20-websites
11 https://www.runews24.ru/society/17/08/2022/a66e4f36646d32e3bb459604947b3390?
12 See recommendations for cybersecurity measures on the Estonian Information System Authority (RIA) website at https://www.ria.ee
13 https://www.ria.ee/kuberturbe-nouanded/nouanded-asutusele-ja-ettevottele/teenusetokestusrunde-ennetus

BELARUS AS A FOOTHOLD IN THE UKRAINIAN CONFLICT

Contrary to Russia's wishes, Belarus has not sent its army units to Ukraine.

By supporting Russia morally, materially and logistically, including by allowing the free use of its territory for manoeuvres and strikes against Ukraine by Russian forces, Belarus hopes to reduce Russian pressure to intervene militarily in the war in Ukraine.

The Belarusian Army's direct involvement in the Ukrainian conflict would be a political gesture with no significant strategic impact on the course of the war.

In January and February of 2022, units of Russia's Eastern Military District arrived on the territory of Belarus as part of the Union Resolve exercise, which was an unexpected and unusual step in the context of Russian-Belarusian military cooperation. The large-scale Zapad exercise had ended in the autumn of 2021. While units of the Russian 1st Guards Tank Army have previously been in Belarus as part of the Russian-Belarusian combined Zapad and Union Shield exercises (they form the Regional Grouping of Forces with the Belarusian army in times of crisis or war), units of the Eastern Military District had no previous contact or cooperation experience with the Belarusian Armed Forces. Also, no one had heard of the Union Resolve exercise.

Since the Kyiv operation, the Russian army has enjoyed complete freedom of action and movement on the territory of Belarus.

All this took place while Russia was massing strike units along the Ukrainian border amidst a general atmosphere of preparing for war. Belarusian representatives promised the exercise posed no threat to Ukraine and that all Russian units would leave Belarus after its end. However, the exercise was just a smokescreen – in the early hours of 24 February, Russian manoeuvre units entered Ukraine from Belarus and launched an attack on Kyiv. This probably came as a surprise even to the Belarusian leadership, as the Kremlin kept Alyaksandr Lukashenka in the dark about its real plans until the very last moment. The attack on Kyiv stalled and ended with the retreat of Russian units to Belarus and their relocation to a new operational area in eastern Ukraine in April. After the Russian manoeuvre units left, some military aircraft and air defence systems stayed in Belarus.

Since the Kyiv operation, the Russian army has enjoyed complete freedom of action and movement on the territory of Belarus. The Gomel region of Belarus, bordering Ukraine, essentially became a large Russian logistics and supply base during the operation. In addition, Belarus provided extensive logistical support to Russia: it allowed the use of its railways and airfields, repaired damaged equipment, treated the wounded, and supplied fuel and food. At the same time, the export of ammunition from Belarusian arsenals to Russia began in March and continues even now. In the autumn of 2022, Belarus also began to supply Russia with T-72 tanks. According to our information, Russia's Defence Ministry also demanded that Belarusian experts be sent to Russia to repair equipment damaged in the war in Ukraine.



Belarus as a foothold in the conflict in Ukraine as of January 2023.

Alongside materiel and logistics, Belarus also supports Russia's activities in Ukraine in the public information space. This is an inexpensive way for Lukashenka to demonstrate his loyalty to Vladimir Putin. The Belarusian leader's speeches contain aggressive anti-Western rhetoric and constantly draw attention to the country's contribution to protecting the border of the Union State of Russia and Belarus. The Belarusian media borrows news reports on the war in Ukraine from the Russian media and broadcasts these unchanged.

Despite pressure from Putin, the Belarusian Armed Forces have not intervened in the military operations in Ukraine and do not wish to do so in the future. The war is unpopular in Belarusian society, and reports of high casualties at the front reinforce this attitude. Belarusian Armed Forces largely rely on conscripts, and sending them to war would threaten the regime's stability. The proportion of professional (contract) soldiers is smaller than in the Russian Armed Forces; the training and equipment are rather poor. Lukashenka cannot be sure that, if sent to Ukraine, his contract soldiers would not desert or join the Belarusian volunteers fighting on the Ukrainian side. Announcing a mobilisation in Belarus carries even greater risks for the regime's security – those called to arms may turn against Lukashenka.

Putin can put pressure on the Belarusian leadership up to a point, but the collapse of Lukashenka's regime would also threaten the Kremlin. Given Russia's engagement in Ukraine, Putin is probably not interested in creating political chaos in Belarus. However, it is possible that Lukashenka will eventually be forced to send troops into Ukraine if the pressure from the Kremlin becomes too strong to withstand.

Putin can put pressure on the Belarusian leadership up to a point, but the collapse of Lukashenka's regime would also threaten the Kremlin.

In October 2022, Russian mobilised troops arrived in Belarus for training. Lukashenka can present this to the Kremlin as another contribution to the war effort while avoiding direct involvement. At the time of compiling this report, the Russian mobilised units in Belarus do not pose a direct threat to Kyiv; however, their presence in Belarus forces Ukraine to deploy some of its units to the north, pulling them away from other fronts.

The use of Russian mobilised units for a new attack on Ukraine from the north would result in heavy losses for the Russian forces. Their progress would be hindered by the mobilised troops' low motivation and training, as well as the Ukrainians' preparedness for an attack from the north. The Belarusian army's involvement in the Ukrainian conflict would be a political gesture without significant strategic impact on the developments on the ground. However, it would still tie up some of Ukraine's forces.

RUSSIAN ADMINISTRATION IN THE OCCUPIED TERRITORIES OF UKRAINE

Russia's annexation of the occupied territories in October 2022 indicates that it has no intention of voluntarily returning them to Ukraine in the future and is ready for a prolonged confrontation with Ukraine and the West.

The fake referendums on joining Russia were passed off as the will of the people remaining in the occupied territories, although the results were known well in advance.

The Russian-occupied areas are undergoing severe regression – they are being Russified and stripped of local resources. The new authorities take no interest in local life and people.

In the spring of 2022, Russia captured a large part of the Kherson Oblast and more than half of the Zaporizhzhia Oblast. With this, Russia secured a land connection with Crimea and moved closer to the goal of gaining control over the entire northern shore of the Black Sea. The quickly appointed occupation authorities, either local or sent in from Russia, began to establish what is known as the "Russian world" (*Russkiy mir*) in the conquered territories, destroying everything representing Ukraine. Preparations started for holding referendums on joining Russia, but this was not considered urgent in the first half of September.

The Russian special services, especially the FSB, play an essential role in establishing and maintaining occupation regimes.

However, the Ukrainians' successful counteroffensive in the Kharkiv region in mid-September changed the calculus for the Russians. They realised the need to quickly incorporate the territories in southern Ukraine to avoid similar failures repeating. After fake referendums staged in late September, Kherson and Zaporizhzhia oblasts and the so-called Donetsk and Luhansk people's republics were incorporated into Russia. Russia did not clearly define the borders of the annexed regions, probably in a deliberate move to retain some leeway for deciding when to declare that Russian territory has been attacked.



A "referendum" carried out the Russian way on 25 September 2022.

Source: Stringer / EPA

The Russian special services, especially the FSB, play an essential role in establishing and maintaining occupation regimes. FSB officers placed in leadership positions in the "military-civilian administrations" organise the occupied territories' integration into Russia according to Moscow's instructions. They curate local collaborators and have a significant say in personnel decisions. In the long term, the plan is to transfer power to civilian authorities loyal to Moscow, but the problem is the scarcity of suitable and reliable collaborators and the Kremlin's distrust of them. Therefore, many positions are filled with Russians or locals who are completely unknown to the residents.

Operative groups of Russian special services officers are also deployed in the occupied territories, among other things, to hunt down Ukrainian patriots and agents and gather intelligence. The same methods were used in the Ukrainian territories that came under Russian control after 2014 when the Donbas authorities and security agencies were managed through curators and special services operative groups appointed by Moscow.

The Russians are experiencing difficulties finding officials willing to work in occupied territories amidst or near hostilities. Personal safety is likely the primary concern. Specialists for reconstruction work are hard to come by, and companies that have started working in the area fear sanctions. Higher wages than usual are offered to attract people to the occupied areas.

The situation of the local leadership and residents is a secondary concern for Russia. The occupation authorities complain that applying for Russian passports is difficult, banks do not work, there is a lack of teachers, and only "Ukrainian propaganda" is broadcast on television. There is also a shortage of medicines and fears about coping in the winter.

Russia's ability to assert itself in the occupied territories has proven to be as deficient as its overall capability to threaten Ukraine.

The Kremlin has long planned the illegal annexation of the territories conquered from Ukraine. The Ukrainians' fierce resistance has stopped Russia from occupying all the desired territory. Moreover, the occupiers did not find the expected support among the local population. On the contrary, the Ukrainians living in the occupied territories have defiantly continued to resist or are looking for ways to leave. Not much effort was made to simulate the legality of the fake referendums organised in haste to legitimise the Russian occupation authorities. Russia's ability to assert itself in the occupied territories has proven to be as deficient as its overall capability to threaten Ukraine.



CHAPTER 2

RUSSIAN FOREIGN POLICY

24

NCD008FY23023_000000388

‘REGROUPING’ OF RUSSIAN FOREIGN POLICY

The demands Russia presented to NATO and the US on 17 December 2021 indicated its long-term goal of changing the fundamentals of European security. Defeating Ukraine is an essential prerequisite for this.

Putin is focusing on creating a geopolitical coalition of authoritarian regimes whose common ground is to oppose the West, democracy and the rule of law.

The invasion of Ukraine ended the Russian foreign ministry’s hopes of playing a meaningful strategic role in the country’s foreign policy planning.

THE WAR IN UKRAINE AND THE EUROPEAN SECURITY ARCHITECTURE

Russia’s full-scale war of conquest in Ukraine, which started in the early morning of 24 February 2022, shook the status quo of European security and is part of Putin’s broader goal of reshaping the European security architecture.

Putin revealed his real objectives on 17 December 2021 when Russia submitted a draft security agreement to NATO and the US, listing demands to change the fundamentals of European security, which also included Ukraine. The most important points were:

1. ending NATO’s “open door” policy
2. rolling NATO’s military deployment back to the 1997 line

On 24 February 2022, Putin began implementing his objectives with a full-scale military attack against Ukraine. Putin likely sees defeating Ukraine as a prerequisite for achieving his broader goals. Russia expected to defeat Ukraine in a matter of days. Things turned out differently because Russia had miscalculated. Russia’s systemic weaknesses – constant lying and stealing within the state apparatus – painted a false picture of the situation in Ukraine for the Russian leadership.

The demands presented to NATO and the US indicate Russia’s long-term goal of reshaping the European security environment into one where NATO would not have a leading role. With this in mind, the military pre-positioning of NATO allies in Eastern Europe, their immediate combat readiness, logistics and supply continuity is of utmost importance.

By now, Putin has made it very complicated for Russia to exit the war – from a foreign policy perspective, by illegally annexing regions of Ukraine, and in domestic policy terms, by declaring mobilisation in the country. Ukraine’s political and military capitulation remains Putin’s objective, and he will go as far as he is allowed to achieve it.

But the time frame has changed: a quick regime change has turned into a long war of attrition, with possible periods of low-intensity military action. In our assessment, Putin believes that Ukraine's resilience and Western support will break before Russia will. Still, in Putin's opinion, Ukraine has not yet currently suffered enough to reach breaking point. Part of Putin's defeat strategy is to systematically damage Ukraine's energy infrastructure during winter, and the goal is to destroy it. Continued military and economic aid from the West to Ukraine is therefore vital to avoid a humanitarian disaster for the civilian population, prevent new crimes against humanity, and ensure Ukraine's survival as a democratic state. European security in the medium term directly depends on the Ukrainians' will to determine their own future and Western unity in supporting Ukraine with all necessary means.

Ukraine's political and military capitulation remains Putin's objective, and he will go as far as he is allowed to achieve it.

According to our information, Russia is not ready to give up the territories it has occupied. It expects an exhausted Ukraine to sit at the negotiating table eventually. Once there, Russia expects to be able to present its conditions and, as a strong negotiator, come out of the situation on the winning side.



The 'Russian world' arrives in Mariupol. A theatre building in the city, where hundreds of civilians had taken refuge from the fighting, was hit by an aerial bomb.

Source: Satellite image ©2022 Maxar Technologies / AFP

According to our sources, Western unity in imposing sanctions has been an unpleasant surprise to the Russian leadership. Those under sanctions seek to use their connections in the West to get off the list, while those threatened with sanctions try to stay off the list. Russia wants the sanctions to end. The sanctions imposed on Russia are not inconsequential but directly affect Russia's ability to maintain its war machine and keep its economy functioning.

REGROUPING OF RUSSIAN FOREIGN POLICY

Russia's losses in the war with Ukraine and its course for a long-term confrontation with the West will force Russia to accelerate a reorientation of its foreign policy. Putin is at war not only with Ukraine but with the entire Western value system as he is convinced that the future of international relations belongs to authoritarian regimes that divide global spheres of influence between themselves, including by using military power. According to the information available to EFIS, Russia is diverting its diplomatic resources from the West to focus its activities on other parts of the world. Undermining Western unity, including unity in imposing sanctions, remains Russia's main goal towards the West.

RUSSIAN FOREIGN MINISTRY'S DRESS CODE

The Ministry of Foreign Affairs of Russia has established rules on the proper appearance of its officials and on "creating a harmonious look".



Impeccably dressed but distracted by journalists, Sergey Lavrov has put his hands in his pockets.

Source: Russian Foreign Ministry Press Service via AP

The requirements for men are conservative - a dark blue or grey suit, with combinations of different jackets and trousers allowed, but only as long as the colours match. Pockets are purely decorative and not to be used for hands. Perfume must be used in moderation; hands and nails must be well groomed. No visible tattoos or piercings are allowed.



Breaking the rules: Maria Zakharova's dress appears to be shorter than allowed.

Source: Russian Foreign Ministry

The requirements for women are also conservative but more detailed. A female employee must have a conservative hairstyle appropriate for her age and position; longer than shoulder-length hair must be neatly styled, and dyeing in unnatural shades is prohibited. Daytime make-up must be understated, foundation must be applied in moderation, and bright make-up at work is inappropriate. Excessive mascara is prohibited, and skirt hems must be 5 cm above or below the knee.

Putin has his stakes on creating a geopolitical coalition of authoritarian regimes opposed to the West who mistrust Western policies and may take a stance against democracy and the rule of law. Russia sees the BRICS nations, the Shanghai Cooperation Organisation members, and several Persian Gulf countries as promising partners. Its focus is on Iran and China, but anyone with historical, ideological or other conflicts

with the West is welcome to join. Russia's goal is to shift the common ground from political declarations and economic cooperation to military cooperation. Moderate success has been achieved – for example, cooperation between Russia and Iran for the weapons used against Ukraine. Russia will probably succeed in bringing other countries on board in 2023. Still, the expansion of Russian cooperation is hampered by the economic ties of the rest of the world with Western countries and their wider geopolitical and economic interests. Nikolai Patrushev, the secretary of the Security Council of Russia, plays a leading role in expanding Russia's security political ties, and he actively travels around Asia and the Middle East for this purpose. Russian officials and politicians also work daily, both bilaterally and in international organisations, to undermine the West, fight against Russia's isolation and sanctions, and expand and deepen global cooperation.



Nikolai Patrushev on a visit to Iran, 8 to 10 November 2022. Russia negotiates an arms deal with Iran that includes weapons to attack critical infrastructure in Ukraine.

Source: IRANIAN PRESIDENCY / AFP

'CANCELLATION' OF RUSSIAN DIPLOMACY

Russian diplomats' role in the West is reduced to a monotonous repetition of propaganda lies.

EFIS has witnessed how the invasion of Ukraine ended the Russian foreign ministry's hopes of playing a meaningful strategic role in the country's foreign policy planning. At least as much as the international community, Russian diplomats were also kept in the dark about Putin's plans to attack Ukraine. According to our information, they found out about it on the morning of 24 February through the media. Confusion and bewilderment ensued, with no one having prepared any talking points in advance. Some decided to switch sides, but the vast majority succumbed to mental resignation and then acceptance, which in some cases turned into angry outbursts of patriotism. Russian diplomats' role in the West is reduced to a monotonous repetition of propaganda lies. Russian ambassadors, finding themselves in an information blackout, are regularly forced to improvise at international meetings. Since 24 February, Russian diplomats' new daily concerns include the anxiety of not knowing whether they will receive their monthly salary in their bank account or, if not, which colleague to borrow money from. Considering the shift of Russian foreign policy towards the Global South, Russia's diplomacy efforts may gain some new impetus in the near future but are likely to end in disappointment. In our assessment, the South and East cannot replace the West for Russia.

A PAPER TIGER IN THE CAUCASUS

Moscow and the Collective Security Treaty Organisation (CSTO) ignored appeals for help from an official ally.

The credibility of Russia's military deterrence in former Soviet territory has weakened.

The reason is the engagement and inefficiency of the Russian Armed Forces in Ukraine.

In September 2022, intense fighting broke out in the South Caucasus between Armenia and Azerbaijan. For almost two days, from 12 to 14 September, the Azerbaijani armed forces launched indirect fire attacks on targets deep inside Armenian territory, including towns and small settlements. Meanwhile, Azerbaijani units crossed Armenia's internationally recognised border and moved several kilometres into the country's territory.

In the September 2022 clashes, Azerbaijan openly attacked Armenian sovereign territory for the first time.

Since the late spring of 2021, numerous armed clashes have occurred between Armenia and Azerbaijan. But the conflict of September 2022 differed from previous clashes in one important aspect: for the first time, Azerbaijan openly attacked Armenian sovereign territory. Both during the Second Nagorno-Karabakh War (from September to November 2020) and since, Azerbaijan has always denied attacking targets in Armenia and claimed that its armed forces had not crossed the internationally recognised state border.

The main reason for Azerbaijan's caution was most probably Armenia's strategic alliance with Russia and its CSTO membership. Formed in 2002, the CSTO, in its current format, is a Russia-led organisation that has been touted for years by Moscow as one of the main security guarantors on the territory of the former Soviet Union. As a kind of "NATO of the East", CSTO security guarantees are triggered if any of its member states are attacked, which is when the other member states – primarily Russia, of course – should come to the aid of the victim of the attack.[1]

During the Second Nagorno-Karabakh War, Russia and the CSTO rejected Armenia's official appeals for help specifically on the grounds that Armenian sovereign territory had not been attacked – the hostilities took place on Azerbaijan's internationally recognised territory.

1 CSTO members are Russia, Belarus, Armenia, Kazakhstan, Kyrgyzstan and Tajikistan.



Russia alone fits under the "umbrella" of Russia's security guarantees. Vladimir Putin is waiting to meet Armenian Prime Minister Nikol Pashinyan on the steps of his residence in Sochi on 31 October 2022.

Source: Sergei Bobylev / AP

During the Second Nagorno-Karabakh War in 2020, Russia and the CSTO rejected Armenia's requests for assistance specifically on the grounds that Armenian sovereign territory had not been attacked.

In September 2022, Armenia also submitted a formal request for assistance to the CSTO. This time, the violation of Armenia's internationally recognised borders was obvious. In response, the organisation did not send weapons or troops to Armenia but dispatched a commission of inquiry. Neither did Russia conduct a military intervention on its own to defend its official ally.

The Armenian government then openly acknowledged that the security guarantees offered by Russia bilaterally and the CSTO had proven to be an illusion and ceased to exist. Participants at the CSTO summit in Yerevan in November 2022 were "greeted" by hundreds of Armenian demonstrators in the city streets, with placards calling Russia an enemy and demanding Armenia's withdrawal from the CSTO.

The Armenian government has openly acknowledged that the security guarantees so far have been an illusion and have ceased to exist.

Two main conclusions can be drawn from the reaction of Russia and the CSTO to the September 2022 clashes in Armenia.

First, the credibility of Russia's military deterrence in the South Caucasus and in the wider area of the former Soviet Union has significantly reduced, at least for the time being. The reasons for this are: (1) the Russian armed forces and military capabilities' engagement in Ukraine and (2) Russia's failure to achieve convincing military success in its aggression against Ukraine.

Second, the security guarantees offered by Russia bilaterally and within the framework of the CSTO have proved to be merely declarative. Russia intervenes militarily to defend its "allies" only when it is in its interest. But not when the alleged allies need help or when a treaty would require to do so. However, the CSTO has turned out to be a "paper tiger": a chatroom, not a serious defence organisation.

These two conclusions have very likely been drawn not only among Armenian leaders but also in the capitals of all other CSTO member states.

RUSSIA'S AFRICAN POLICY

Increasingly affected by the sanctions imposed by Western countries, Russia has intensified its efforts in Africa to project itself as a geopolitically active great power.

Russia hopes to achieve rapid diplomatic and economic success with the cheapest possible means; however, in reality, it lacks the capacity to fully implement its plans in Africa.

Russia sees itself as having the greatest potential as a provider of security services in Africa and focuses on politically unstable countries that provide Russia with opportunities to profit from local natural resources.

RUSSIA'S AFRICAN EFFORTS

Increasingly affected by the sanctions imposed by Western countries in response to starting full-scale hostilities in Ukraine, Russia has intensified its efforts in Africa to project itself as a geopolitically active great power. While Russia's actions aim to sustain that image, its increased efforts in Africa are also due to the matter of fact need to avoid essentially being alone in United Nations votes on matters concerning Russia's aggression against Ukraine. In this latter goal, Russia has not succeeded. Nevertheless, Russia continues to try to reduce Western influence and redefine the balance of power in Africa. Russia is looking to Africa for a success story, for allies and for support for its anti-Western activities and narratives. It hopes to achieve quick diplomatic success in African countries with the cheapest possible means by providing security services to them to gain control over them and make them dependent on Russia to profit from the rising opportunities down the line.

Russia is looking to Africa for a success story, for allies and for support for its anti-Western activities and narratives.

Russia's interest in Africa increased several years before the full-scale military attack on Ukraine. The first Russia-Africa summit in Sochi in 2019 falls into this context. The event received extensive media coverage as Russia promised to double its trade with African countries in five years. However, since then, the volume of Russian trade with African countries has decreased from 20 billion US dollars in 2018 to 17.6 billion dollars in 2021. Russia overestimates its role and influence and lacks the capacity to implement its plans in Africa fully. Although Russia's endeavours were probably somewhat hampered by the coronavirus pandemic that started at the end of 2019, they are mainly set back due to intense competition. China meanwhile managed to increase trade with African countries by 35 per cent, to a record 254 billion dollars in 2021.

Despite the setbacks, the Russian leadership sees the situation in Africa as favourable for Russia and tries to expand its foreign policy levers by developing cooperation with African countries in multilateral and bilateral formats. Russian representatives in Africa are looking for opportunities to gain popularity by presenting themselves as a helpful and reliable partner with friendly rhetoric. According to the information available to us, Russia plans to expand its network of diplomatic missions in Africa, increase its diplomatic staff, simplify currency transactions with African countries and diversify payment methods. To implement these plans more efficiently, Russia plans to expand its membership in organisations. For example, it has expressed interest in obtaining observer status in the African Parliamentary Union.

IN ANTICIPATION OF THE NEXT RUSSIA-AFRICA SUMMIT

The next summit between Russia and Africa is planned to occur in Saint Petersburg in the summer of 2023. Organising the summit has not been without problems, and the event has been postponed several times. Originally scheduled to take place in 2022 in Addis Ababa, then in Sochi, and even as a video conference, the summit will finally take place in Russia, as sanctions make it difficult for the Russian delegation to travel to Africa. Coordinated by the Russian foreign ministry, the preparations for the summit were not particularly productive. The organising committee has been working under the direct authority of President Vladimir Putin to avoid further setbacks, led by his adviser Yuri Ushakov, since July 2022.

Since the beginning of the full-scale attack on Ukraine, Russia, which intends to treat food security as a priority topic at the summit, has systematically spread and exploited false claims about the critical situation of world food security and Western sanctions' negative impact on it. With the help of this narrative, Russia amplifies the international community's fears and props up its proposals for at least a partial lifting of the sanctions. Accusing the West of damaging Africa with sanctions, the Russian leadership, including President Putin and Foreign Minister Sergei Lavrov, call on African countries to put more pressure on Western countries to ease sanctions that inhibit trade (e.g., fertilisers) and push them to spread rhetoric that suits Russian interests.

Shipments of fertiliser and grain are promised in return and, if necessary, credit to pay for these. However, according to information available to us, the communication between Russian representatives, who present themselves as a helpful partner, gives a more vivid picture of their real attitude towards the representatives of African countries. If negotiations do not proceed quickly enough, Russian representatives humiliate their supposed partners, use racist language and complain that "your hair will turn grey or you might die before you beat a contract out of them".

RUSSIAN SECURITY COOPERATION FOCUSES ON THE SAHEL, ESPECIALLY MALI

Competing with Western countries, Russia sees Africa's greatest potential in the security sector. Russia focuses on politically unstable countries that need help to guarantee their security and simultaneously provide Russia with opportunities to profit from local natural resources. The Sahel is one such region where the security situation is complicated and military coups have taken place in several countries (Guinea, Burkina Faso). Mali has asked Russia for help to step up the fight against terrorism. Due to political instability and

a difficult security situation in Mali, Russia has managed to intensify cooperation with the country. Mali is offered security expertise with the support of private contractors, thus enhancing Russia's image as a crisis solver and gathering support for anti-Western activities and narratives.

Russia's focus is on politically unstable countries that need help to guarantee their security and, at the same time, provide Russia with opportunities to profit from local natural resources.

Mali and other countries in the Sahel region can expect little real benefit from security cooperation with Russia. So far, the security situation in Mali has worsened significantly during its intensified cooperation with Russia. Being engaged in Ukraine, Russia lacks the capacity to increase its financial, military and political contribution to Africa and sustainably conduct counter-terrorism operations in Mali or elsewhere in the Sahel. To improve the security situation and sustain the fight against terrorism, Russia should support the Malian army with large forces at a wider regional level, also bringing in civilian staff. Despite its limited capability, Russia will likely continue to take advantage of opportunities opening up in Mali and elsewhere in Africa to discredit the activities of Western countries on the continent. By amplifying the anti-Western narrative, Russia further tenses up the situation, both in specific African countries and on the continent as a whole, without offering real solutions or helping to improve the security situation.

WAGNER: AN INSTRUMENT OF RUSSIAN STATE POWER IN AFRICA

Russian private military companies are an increasingly important tool for Russia in pursuing its geopolitical goals. Among them, Wagner has received the most public attention. Associated with Russian oligarch Yevgeny Prigozhin, Wagner has been active in many different parts of the world, from Venezuela to Ukraine, where the group is currently actively involved in military operations. Wagner has focused on Africa since 2015. Its presence has been observed in Libya, Madagascar, Mozambique, the Central African Republic, Sudan and, since 2021, Mali – a country to whose security Estonia has also directly contributed.

Wagner is a useful geopolitical tool for Russia in two ways. On the one hand, using private military companies allows the Kremlin to pursue its policies without demonstrating too much official involvement. On the other hand, Wagner's operations bring economic opportunities for companies connected to various Russian oligarchs.



According to our information, the equipment delivered from Russia to Mali broke down within a year; only one out of eight attack helicopters (Mi-35M, Mi-171) was operational at the end of 2022. According to the Russian representatives, the equipment broke down due to the incompetence of Malian personnel.

Source: French Armed Forces via AP



Despite the seemingly warm relations between the foreign ministers, cooperation with Russia and Wagner has not brought Mali the expected results.

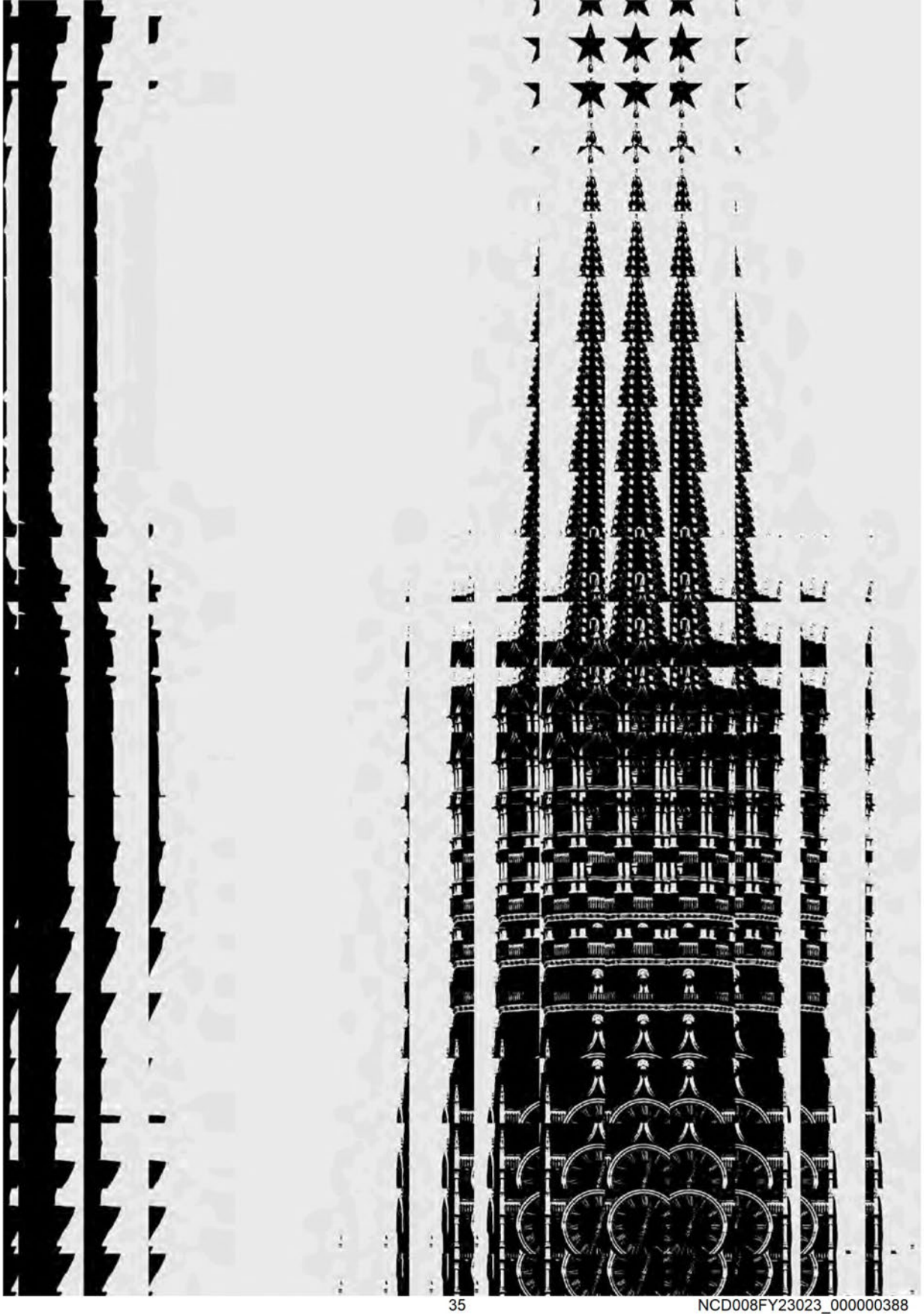
Source: Russian Foreign Ministry via Reuters

Wagner generally uses the same modus operandi. As the first step, diplomatic and military cooperation is strengthened between Russia and the target country. This is followed by agreements on the export of military equipment and, finally, the hiring of Wagner. Mercenaries often arrive in the country under the guise of military advisers or instructors. At the same time, a suitable environment is prepared through information operations discrediting previous security partners and glorifying Russia's ability to ensure stability in the country; potential funding sources are mapped, such as mineral deposits.

Wagner mercenaries arrived in Mali at the end of 2021. Wagner's activities in Mali have not improved the security situation in the country. On the contrary, terrorist attacks and violence against civilians have increased, especially in central Mali, where Wagner and the Malian armed forces have mainly conducted their operations. Wagner's mercenaries have been repeatedly accused of human rights violations and crimes against humanity. In addition, Wagner members have tried to falsify evidence to suggest that French troops have committed mass murder in Mali. French and other Western troops have left Mali. This has left a security vacuum, which Wagner has not been able to fill and almost certainly will fail to fill in the future. The fate of Mali is likely to be the same as the other African countries where Wagner has arrived to ensure security: the promised stability will not be achieved, and the situation will only worsen.

Kremlin will very likely want to continue using private military companies to pursue its geopolitical ambitions in Africa.

Russia's full-scale attack on Ukraine has also left its mark on Wagner's activities. The war has not gone in the direction the Kremlin wanted. This has led to a situation where Wagner's former veil of secrecy has fallen. Fighters are recruited publicly through advertisements, and Prigozhin, who personally visits Russian detention facilities to recruit personnel, has finally confirmed his links to Wagner. Kremlin will very likely want to continue using private military companies to pursue its geopolitical ambitions in Africa. Russia's lack of military personnel in Ukraine has led Wagner to withdraw its fighters from Libya, the Central African Republic and even Syria. As the situation worsens, Wagner may also leave Mali. In this way, Russia leaves others to resolve the problems and further deepens instability in the entire region.



CHAPTER 3

RUSSIAN DOMESTIC POLITICS AND ECONOMY

36

NCD008FY23023_000000388

RUSSIA'S DOMESTIC POLITICAL SITUATION

Putin's regime is rapidly moving towards an open dictatorship. As the country is at war, the last vestiges of democratic government have been abandoned, and any dissent qualifies as a crime.

In the coming years, the current regime led by Putin, or a slightly modified but equally undemocratic and coercive updated version, will most likely continue to hold power in Russia.

Russia's transformation into a stable democracy is unlikely in the coming years.

THE DOMESTIC POLITICAL SITUATION AND THE FUTURE OF THE REGIME

Even if a rather unlikely scenario were to materialise and see the Russian regime collapse, paving the way for democratic elections, any attempts at democratisation would very likely be short-lived.

The events of 2022 convincingly demonstrated the autocratic and undemocratic regimes' great potential for aggression and their negative impact on regional stability and general security. Unfortunately, the trends in Russia's operating principles and domestic political situation are unlikely to lead to the country's transformation into a stable democracy in the near future. Even if a rather unlikely scenario were to materialise and see the Russian regime collapse, paving the way for democratic elections, any attempts at democratisation would very likely be short-lived, similar to previous such attempts in Russia. It must be taken into account that the official ideology, which stokes Soviet nostalgia and neo-imperialist ambitions, obstructing the objective treatment and reassessment of Soviet history, has left a strong mark on Russian society. At the same time, society's expectations and attitudes are largely shaped by a lack of democratic experience and the negative experience of the 1990s.

In the coming years, the current regime led by Putin, or a slightly modified but equally undemocratic and coercive updated version, will most likely continue to hold power in Russia. However, the continuation of a Putinist regime will not guarantee domestic political stability – internal tensions will inevitably intensify, and the power struggle among the Russian elite will deepen in the near future. Putin's age is one factor driving the internal struggle for power as the question of a successor becomes increasingly

urgent. The situation in the government is even more strained with the unsuccessful war against Ukraine. The prospect of losing the war prompts those in power to look for scapegoats in their ranks to point fingers and save their own skin. A sudden power transition in Russia is possible in case a military defeat in Ukraine becomes inevitable – the likelihood of this scenario, however, is very low.

The economic situation, which is becoming more and more complicated due to sanctions, and the mobilisation, which has received a largely negative response among the population, aggravate the situation on the home front. The country's economic resources are shrinking, and the struggle between different interest groups for funds redistributed from the state budget is intensifying. Those who have proven themselves to the Kremlin as efficient and loyal managers and are better at divining the leader's intentions have been more successful in this struggle.

ATTEMPTS TO CREATE A NEW RUSSIAN STATE IDEOLOGY

Putin's regime is rapidly moving towards an open dictatorship. As the country is at war, the last vestiges of democratic government have been abandoned and any dissent qualifies as a crime. At the same time, the Kremlin has realised that the lies used to justify the war in Ukraine rest on shaky foundations and it is very difficult to explain the increasingly radical methods to the Russian public. Although laws have been passed to ensure that "true" information is issued from a single state-controlled source, it is unrealistic to impose a complete information blockade on the population in today's world. The Kremlin launches propaganda campaigns, clearly modelled on those used in the Soviet Union, to justify the war and deepening dictatorship. Starting from September 2022, a mandatory patriotic education programme, known as "Conversations About What Is Important", has been launched at all levels of education in Russian schools. The purpose, according to the brief, is "to develop students' understanding of Russian history, traditional patriotic values and their duties as citizens of a united, multi-ethnic country". But this is just the beginning. The Kremlin has announced that in 2023 a new special ideological course, "Foundations of Russian Statehood", will be launched in universities, curated by the Presidential Administration's domestic policy directorate. According to the Russian media, the course materials are prepared by well-known anti-Western and nationalist conservative researchers and lecturers who are extremely loyal to Putin. The main goal is to explain Russia's special development path and historical mission in establishing a new "multipolar world order".

THE RISE OF RADICALS

Russia's elite seems to be no stranger to the idea that the increasingly irremediable situation could be resolved by a "rebranding" of the regime, presenting a liberalised system domestically and internationally after making certain changes. However, this could only work at the price of replacing Putin, even if any other changes are insignificant. Given the threat of such scenarios, it is crucial from a Western perspective to clearly distinguish between an actual and apparent liberalisation of the system.



Ramzan Kadyrov, Head of the Chechen Republic, represents the radical faction of Russia's ruling elite.

Source: Chingis Kondarov / Reuters

Currently, an even more radical faction is rising to the fore in Russia's ruling elite, and some previously more moderate members of the elite have started to stand out with rather extreme statements. Their behaviour may be a sign of panic; they may have realised that the war in Ukraine was a huge mistake that can no longer be corrected, and the only way forward is to struggle on, using increasingly radical methods. It is also possible that allowing the radicals to take centre stage is part of Putin's tactics to show that his disappearance would bring an even more extreme group to the helm.

Currently, an even more radical faction is rising to the fore in Russia's ruling elite.

The fear of the regime's image change scenario is a possible reason why Putin relies more and more on radicals like Yevgeny Prigozhin and Ramzan Kadyrov. The reputation of these people (unlike several other members of the Russian ruling elite) would not allow them to be in a leadership role in a regime projecting itself as more liberal. The same kind of reasoning can motivate Putin to arrange for power figures with a previously moderate image to completely discredit themselves with radical statements.

But even if the radicals' rise to dominance in the ruling elite is part of Putin's calculus, it will still have consequences for the regime's present and future. At some point, Putin himself may have difficulty taming people increasingly emboldened by their growing influence, especially if Putin has authorised them to settle scores with their opponents. Prigozhin and Kadyrov are particularly dangerous in this context because each of them essentially has their own private army, from which their usefulness to the Kremlin and an important part of their influence derive.

RELATIONS BETWEEN THE PRESIDENT OF RUSSIA AND KEY AUTHORITIES

Making political decisions in today's Russia is more than ever concentrated in the hands of one person and is, therefore, even more difficult to predict. Decisions made by an ageing autocrat, only considering expert opinions based on personal whims and prejudices, are prone to miscalculation.

The responsibility for implementing Putin's policies and making administrative decisions continues to be centred in the Presidential Administration (PA), whose curating role is even broader in reality than the legal framework stipulates. The PA's top leadership has remained unchanged for years. The chief of staff, Anton Vaino, has apparently proven himself to Putin as a thoroughly loyal and highly efficient administrator. But Putin probably also appreciates Vaino's lack of charm and his ability to stay in the background, so the master of the Kremlin has no reason to fear Vaino might make a play for his chair should favourable circumstances arise. Sergey Kiriyenko, the first deputy chief of staff of the PA responsible for domestic policy, who in 2022 was also entrusted with the civil administration in the occupied territories of Ukraine, is another member of the leadership who has retained the favour of the president. Remarkably, Kiriyenko, who first became known in Russia as a liberal in the 1990s, has taken the regime's increasingly rough politics in stride and seemingly has no scruples about supporting it wholeheartedly..

On the other hand, the Security Council of the Russian Federation (SC) has lost some of its previous influence. Although there are still people in the SC whose views have weight in Putin's eyes, their importance and position in the power hierarchy derive primarily from personal ties with Putin (and the current status of such ties) rather than SC membership. The SC's devalued role was evident at a public session just before the invasion of Ukraine, where Putin, probably quite intentionally, demonstrated that the SC was no longer a serious venue for discussion and decision-making. Rather, the SC has developed into an institution where important decisions previously made in a narrower circle are only formalised, thereby shifting the responsibility for what is happening to the entire political leadership.

THE RUSSIAN ECONOMY

Oil exports and the high price of oil in 2022 have helped Russia withstand the pressure of sanctions. However, in 2023 the sanctions imposed on Russia's oil exports will begin to have an effect. This will lead to a decrease in Russia's oil revenue.

The self-imposed sanctions by international businesses, such as leaving Russia, have hit the Russian economy faster than the sanctions imposed by national regulations.

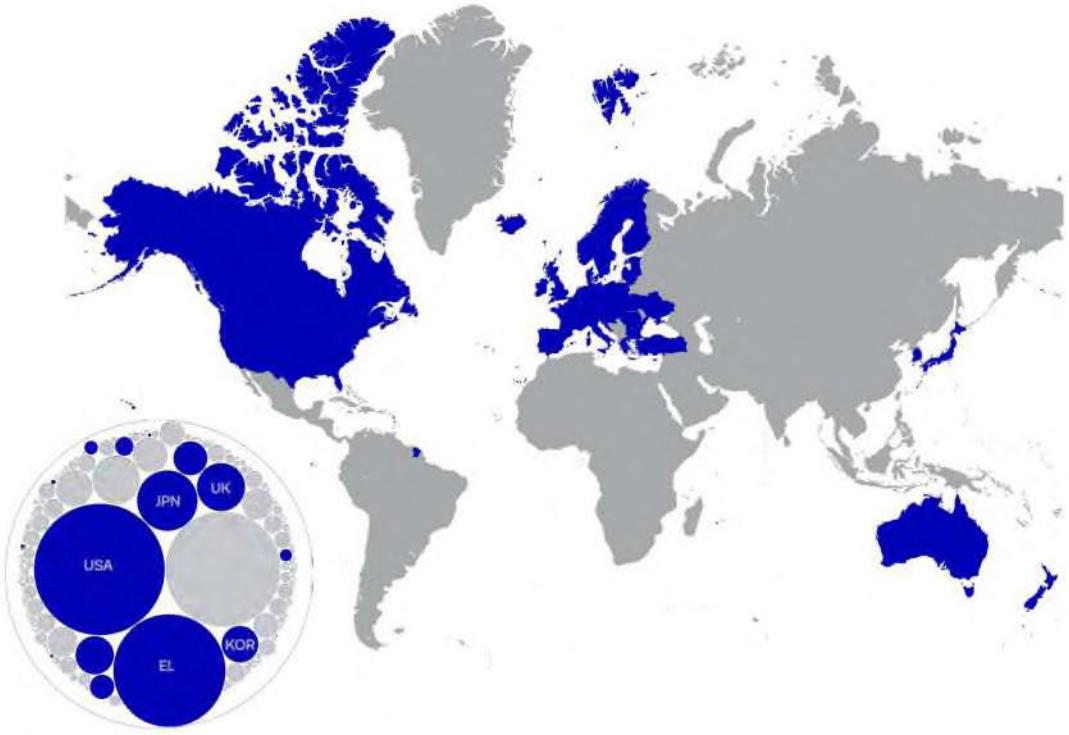
Russia is exploiting the issue of food security to promote the narrative of peace at any price in Ukraine.

From time to time, Western media reports on the state of the Russian economy, citing a slight recession and rather modest inflation. These reports tend to rely uncritically on the estimates of the Bank of Russia or Russia's finance ministry. The sources of these estimates are classified, which makes these forecasts essentially nothing more than propaganda. Making economic assessments is complicated by the fact that due to sanctions, Russia's imports slowed down in the second quarter of 2022, while export volumes were maintained for some time; the combined effect of these two factors has led to a strengthening of the rouble's exchange rate. A paradoxical process occurred when artificial restrictions and measures were combined – the currency gained value while the economy was in recession. Therefore, the macro indicators of the Russian economy should be taken with a grain of salt.

SANCTIONS

Russia's kinetic war in Ukraine, launched on 24 February 2022, has significantly changed the sanctions against Russia. The previous principle of sanctioning *specific persons for specific actions* was replaced by outright sanctions affecting the country's

economy as a whole. Financial sanctions, a ban on the provision of payment services by major banks (or what is known as "exclusion from SWIFT"), a restriction on the purchase of petroleum products and the freezing of foreign reserves are a set of tools with a very strong impact.



Countries that have imposed sanctions against Russia constitute over 60% of the world's economy.

As another important variable, the self-imposed sanctions by international businesses, meaning the avoidance of business with Russia without express legal regulation, have also begun to have an effect. Public opinion has been largely shaped by Ukraine's interpretation of the events, which has been corroborated by the information disclosed by Western intelligence services about Russian attack plans. By the time Russia attacked, Western consumers had a well-developed understanding of who the victim and the aggressor were, that what was happening was a war and not an "operation", and that Ukrainians were fighting for their freedom rather than undergoing an anti-fascist clean-up. The influence of Western consumer sentiment and the realisation of the decline of Russia's business environment has forced businesses to leave, and the consequences of their departure have hit the Russian economy faster than the sanctions imposed by national regulations.

The countries that have imposed sanctions on Russia (EU member states, US, UK, Canada, Australia, Norway, etc.) account for more than half of Russia's current exports and about 60% of the world economy, oil consumption and the global defence budget. Outside the "sanctioning world", there are two major economies – China and India,

representing 18% and 3.3% of the global GDP, respectively – and the remaining 20% consists of many relatively small economies. Although Russian rhetoric strongly addresses the subject of "new markets", no plausible solutions exist for continuing Russia's foreign trade as it was before. The impact of international isolation is deepening, and even in relations with China and India, which are presented as a way out, Russian businesses are being cynically exploited.

The scope of sanctions has changed, and the current modus operandi for avoiding sanctions, which is essentially based on illicit trade, is no longer sufficient, as the number and quantities of goods that need to be hidden have increased. An industrial economy cannot be kept going with ad hoc supply chains and improvised solutions.

FOOD SECURITY AS PART OF AN ANTI-SANCTIONS CAMPAIGN

The war closed the shipping routes out of Ukraine. Before the war, Ukraine was a major grain exporter, supplying corn and wheat mainly to Mediterranean and Middle East countries. Marine transport allows for the cheap and fast export of large quantities of grain (up to 100,000 tonnes per vessel, compared with 60 tonnes in a rail wagon). Ukrainian ports – Odesa, Chornomorsk and Mykolaiv – had the modern infrastructure for receiving grain from rail wagons and quickly transferring the cargo to ships.

Within a few months of the start of the war and the imposition of sanctions, alarming opinions began to spread in the world media, stating that because grain was held up in Ukrainian warehouses due to blocked shipping routes, African and Asian countries would soon starve. Parallels were repeatedly drawn with the Arab Spring riots, which were also allegedly sparked by high grain prices. It is true that the prices of grain, as well as many other commodities, rose sharply after Russia invaded Ukraine, but the world market prices of grain did not remain at the peak level reached at the beginning of the war.

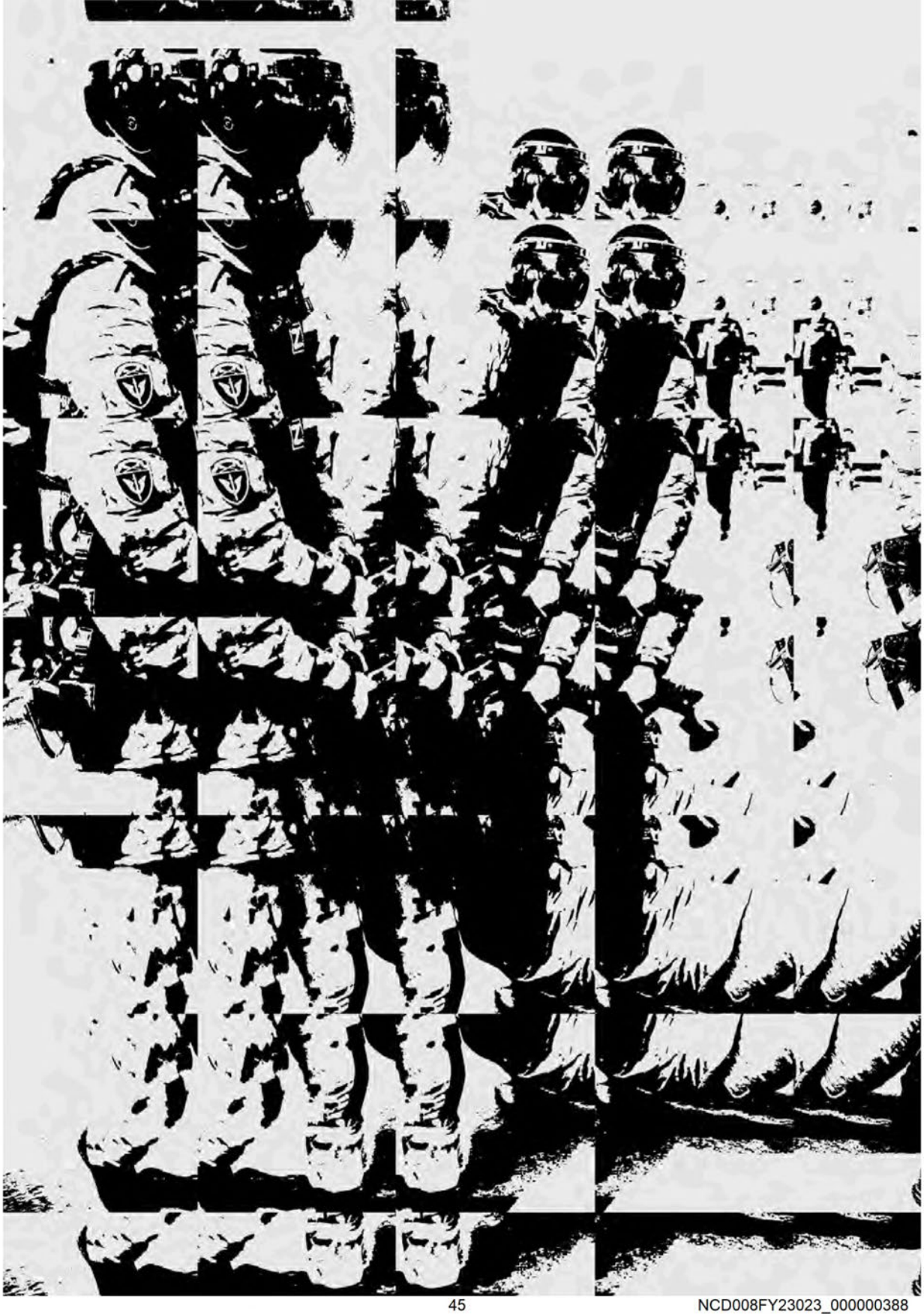
Russia attempted to take advantage of the public concern about food security and to spread an exaggerated narrative about a food shortage.

It should be noted that Russia attempted to take advantage of the public concern about food security and to maximise the spread of an exaggerated narrative about a food shortage. On the one hand, Russia wanted to use this topic to influence the international community. This was probably done in the hope that the prospect of the global socioeconomic effects of a drawn-out conflict would push the West to support peace at any price in Ukraine, prioritising a speedy ending of hostilities over achieving a just and sustainable peace from Ukraine's point of view.

On the other hand, Russia attempted to use food security-related fears to criticise and undermine the sanctions policy. For example, according to the Russian narrative, to compensate for the undelivered grain, EU sanctions on Russian food products and fertilisers, which allegedly would have saved the lives of hundreds of millions of people in developing countries, would have to be removed. Russian diplomats, Western-oriented propaganda channels and several current and former politicians with good connections in EU institutions worked to amplify this narrative. In doing so, they were not distracted by the fact that the EU sanctions do not actually concern

Russian grain or fertilisers. Russia has enough resources and infrastructure to export these goods to third countries without using EU ports. However, *personal* sanctions are in place against several oligarchs involved in fertiliser production with close ties to the Kremlin's power circles, whose profits and lifestyle suffer significantly from the sanctions. The dramatic interviews with them in Western media channels confirm this.

In cynically exploiting the issue of food security, the Kremlin did not limit itself to the above activities. Advancing its interests by exploiting a vital concern for many of the world's poorest countries and by inciting fear, Russia tried to present itself as an advocate for these countries, which are the most vulnerable in the event of a global food shortage.



CHAPTER 4

RUSSIAN SPECIAL SERVICES

46

NCD008FY23023_000000388

COVERS USED BY RUSSIAN INTELLIGENCE SERVICES

Russian intelligence services widely use covers to hide the connections between intelligence operatives and their real employer – the intelligence service.

On Russian territory, intelligence services can use almost any institution, company, or organisation as cover.

Anyone communicating with Russian federal or regional authorities, research institutions, or strategic companies should remember that their international relations, especially with Western countries, are largely controlled by Russian intelligence services.

COVERS IN INTELLIGENCE

A cover (Russian *прикрытие*) is used to obscure the true identity of a person or organisation and hide their affiliation with an intelligence agency.

The most common type of cover used by officers of the Russian intelligence services operating abroad is a diplomatic position in an official Russian mission: an embassy, consulate, or trade mission. The Vienna Convention protects intelligence officers operating under diplomatic cover. If caught, they are declared *persona non grata* in the host country and sent back to their home country.

In addition to "diplomats," operatives active abroad also include "illegals" who may pose as citizens of Russia or another country and work under an assumed identity, for example, in business, research, journalism, or the arts. "Illegals" are not protected by international conventions and can be arrested and prosecuted in the host country if discovered.

In addition to diplomats and illegals working abroad, whose activities have been reported quite often in the international media, all three Russian intelligence services – the internal security service FSB, the foreign intelligence service SVR and the military intelligence service GRU – also use undercover intelligence officers on Russian territory. This chapter is about these officers.

COVERS USED BY RUSSIAN INTELLIGENCE SERVICES ON RUSSIAN TERRITORY

The FSB, SVR, and GRU regularly use covers for intelligence activities carried out on Russian territory.

As one of the pillars of the current regime, Russian intelligence services enjoy extensive support from the authorities and considerable freedom of action. The FSB, SVR, and GRU can use almost any state authority, company, or organisation as a cover when necessary. As a rule, a cover is created in one of two ways.

1. The cover organisation does not engage in intelligence work but pursues its statutory activities (governance, research, business, journalism, etc.) and has one or more positions staffed by intelligence services officers. Most undercover officers work in such positions and, to avoid exposure, must at least partly perform the tasks that would normally be prescribed for their job.
2. An entire organisation is established as a cover for an intelligence service. It does not pursue the activities listed in its articles of association or only does so to a minimal extent to avoid suspicion. Since such organisations are largely fictitious, the officers working there can fully focus on intelligence activities.

The Russian intelligence services have a broad scope of activities – they collect intelligence information but also engage in counterintelligence and fight economic crimes, terrorism, extremism, domestic democratic opposition, drug trafficking, etc. Thus, they also use very different cover organisations and positions. The covers described here have a common denominator – they can all be used to establish contact with foreigners.

Russian intelligence officers work undercover in Moscow and elsewhere in Russia; their number depends on the region and how many foreigners visit it. For example, up to half of the officers of the FSB intelligence units can work undercover at any given time, spending a large part of their working time outside the FSB and visiting the agency only episodically to report back and receive instructions. A cover can be permanent or temporary. An officer working under temporary cover will pose as an employee of an organisation for a short time to carry out a specific task, for example, attending an international conference as a member of a think tank or research institution.

On paper, the identity of intelligence officers should be secret. Still, in many cases, the other employees of the cover organisation can identify them because they just show up with an unknown educational and professional background and have different work duties than the rest of the staff. Intelligence officers are also often discovered when a cover position within an organisation is used continuously, regularly rotating officers in and out.

EXAMPLES OF UNDERCOVER WORK

The covers described here are used by undercover intelligence officers who are responsible for recruiting foreigners.

The FSB often uses the Federal Migration Service (FMS) as a cover. This provides a legal opportunity and a plausible pretext to communicate with foreigners arriving and staying in Russia and ask them questions about themselves, their families, and the purpose of their visit to Russia.

Intelligence officers also hold positions in federal institutions that coordinate cooperation with so-called Russian compatriots living abroad. Russian compatriots are under heightened scrutiny by the FSB's main intelligence unit, the Department for Operational Information (DOI) of the Fifth Service. This scrutiny is characterised, among other things, by the fact that the government committee for Russian compatriots living abroad – the body that coordinates the handling of compatriot-related issues in the state institutions – has always included a DOI senior officer, most recently General Dmitry Milyutin, the deputy head of the DOI. What does the FSB have to do with Russian compatriots, and why should an intelligence unit curate this field within the FSB? The answer is obvious: the FSB needs Russian compatriots living abroad to recruit collaborators from among supporters of the "Russian world"

ideology and have them gather intelligence from their host country and spread propaganda glorifying Russia and discrediting their current homeland and other Western countries.[1] Effectively, the DOI coordinates the preservation and renewal of a fifth column, especially in countries bordering Russia with a large Russian-speaking community.

Russian intelligence services play an integral role in developing and implementing Russian foreign policy in the Baltics, including policies pertaining to so-called Russian compatriots.

The Federal Agency for the Commonwealth of Independent States Affairs, Compatriots Living Abroad, and International Humanitarian Cooperation (*Rossotrudnichestvo*) and its representatives abroad – Russian research and cultural centres – are regularly used by the FSB and SVR as cover for their officers. FSB officers "work" at the Moscow House of Compatriots (*Moskovskii Dom Sootechestvennikov*) of the Government of Moscow. In the Presidential Administration of Russia, the country's most important domestic and foreign policy body, Russia's Baltic policy has long been made under the supervision of SVR and FSB officers working undercover.

All three intelligence services use the international cooperation departments of Russia's central and regional authorities (incl. city and oblast governments) as cover for their intelligence officers. However, the intelligence services also use trustees working there to gather information about the authorities' foreign contacts and international cooperation projects. We can say that the intelligence services largely control the international cooperation of Russian federal and regional authorities.



Spot the spies! On 16-19 November 2022, the 10th forum for so-called Russian compatriots living in the Baltic states was held in Roshchino, Leningrad Oblast. The forum participants included several individuals with ties to the Russian intelligence services; however, they all represented some other institution or organisation.

Source: Vyborg TV (screenshot)

Intelligence officers often work undercover at universities and research institutions, usually in the institution's management or international relations unit, in positions allowing them to keep up with the institution's international contacts, including being informed about students and delegations arriving from abroad. They also recruit researchers travelling abroad to carry out intelligence tasks, such as participating in conferences and research projects to establish contacts with foreign researchers or gathering research and technology-related information, including stealing scientific discoveries. Officers of the Russian intelligence services work undercover in the Russian Academy of Sciences and major universities both in Moscow and elsewhere in Russia.

As "employees" of public and private think tanks and "research institutes," intelligence officers can participate in conferences and seminars attended by foreigners. In addition

1 It should be emphasised that the FSB also recruits people who do not have access to classified information. Such persons are mainly used in influence operations against foreign countries and their population.



The badge of the FSB 5th Service DOI. The badge displays common symbols for the FSB – a sword and a shield. The globe on the forefront is a common symbol for Russian intelligence services units that are responsible for gathering information on foreign countries.

Source: forum.faleristika.info

to profiling foreign participants, they have a significant opportunity to spread views aligned with Russia's political interests through the think tank's publications and personal communication with foreign guests. In other words, they conduct influence operations.[2] Here are some examples:

The Institute of Diaspora and Integration (Institute of CIS Countries)[3], founded in 1996 and headed by Konstantin Zatulin, a member of the Russian State Duma, studies Russia's "near abroad" (which also includes the Baltic countries) and spreads views justifying Russia's aggressive foreign policy. The institute has long had close ties with the FSB and especially the DOI, whose officers have regularly served as aides or advisers to Zatulin. Among them is Valery Solokha, described by the *Dossier Center* in October 2022 as the head of the DOI's sub-unit for Moldova.4 Solokha was succeeded as Zatulin's aide by DOI officer Maxim Sapunov, who previously held posts in the Government of Moscow and the Moscow House of Compatriots. Another aide to Zatulin was DOI officer Maxim Lobanov, whose duties included protecting the interests of the Russian Orthodox Church in Ukraine.

The official mission of the Eurasian Cooperation Development Fund,[5] established in 2012, is "spreading the idea of a Eurasian Union formulated by Russian President Vladimir Putin in the post-Soviet space." In addition to residents of the CIS countries, attempts have been made to involve activists from the Baltic states in the organisation's activities. An FSB DOI officer has regularly staffed the position of vice president of the foundation.

The Russian Institute for Strategic Studies (RISI)[6] operated under the SVR until 2009 and was designated as Military Unit 61360. Although it has since been officially subordinated to the Presidential Administration, RISI has always been led by former high-ranking SVR officers, currently by former SVR director Mikhail Fradkov. Among RISI employees, including the director's team, are SVR officers participating in the institute's foreign communication and international cooperation projects. An example is a conference on the relations between the Eurasian Economic Union and China's Belt and Road Initiative, held in Moscow in April 2021 with the participation of SVR officers.

In our public threat assessment in 2021, we described the organisations established by the GRU for intelligence and influence activities, including the Russian Foreign Institute and the Inforos information agency.

The FSB and SVR also use the organisations of Russian industrialists and entrepreneurs as well as industrial and financial companies' foreign relations departments as cover. This provides Russian businessmen with international business contacts and allows them to spread the message about the importance of good relations with Russia and the necessity of "separating business and politics." of "separating business and politics."

2 In Soviet terminology, influence operations involved influencing key figures and ordinary citizens in other countries in the interest of the Soviet Union. Similar to their Soviet predecessors, Russian intelligence agencies consider influence operations as equally important with intelligence gathering.
3 https://i-sng.ru
4 https://fsb.dossier.center/mid/
5 https://fondres.ru
6 https://riss.ru

THE RUSSIAN SPECIAL SERVICES' SUPPORT TO PRESIDENT PUTIN

During the war in Ukraine, the Russian special services have deliberated and concocted messages to help explain Russia's actions to its citizens and show the president in a favourable light.

The messages justify Putin's actions in Ukraine and create an image of him as an astute leader with foresight but, at the same time, lack objectivity and context and are often subject to public ridicule.

The prevailing view in the Russian special services is that by persistently lying and feeding conspiracy theories, sometimes hinting at the involvement of special services to add mystery, they can continue to speak to a certain segment of society.

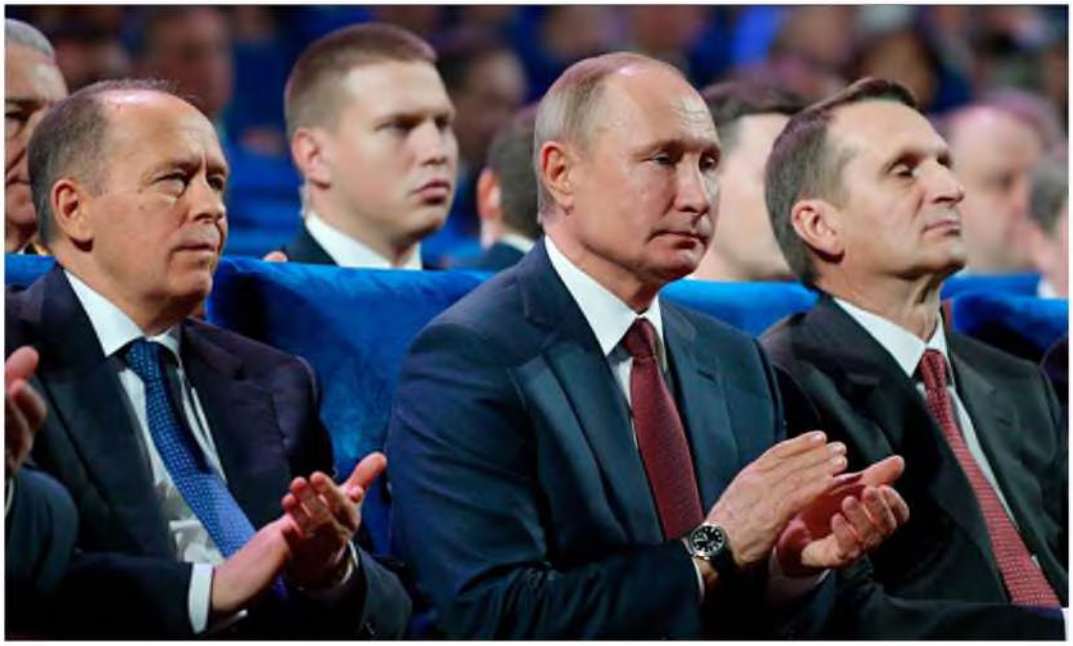
The war in Ukraine has put the Russian special services in an unprecedented situation. The problems they need to address now include the sentiment of Russian citizens. At the same time, they also want to express their loyalty to the country's leadership and President Putin. There was a tense period at the beginning of the war as it became clear that a surprise attack would not succeed. Tensions rose again when a partial mobilisation was announced in September, just a few weeks before the president's 70th birthday..

The intended effect was to convince the audience of Russia's continued great military and economic capabilities and good intentions toward its own people and the Ukrainians.

In September 2022, the Russian special services were still busy gathering ideas for updating the material used to celebrate President Putin's services to Russia. The material includes old talking points praising Putin, previously used in the 2018 presidential election campaign, which have become a laughingstock in the media as they repeat the existing narrative based on questionable statements and outright lies. The intended effect was to convince the audience of Russia's continued great military and economic capabilities and good intentions toward its own people and the Ukrainians.

Here are a couple of examples of the outrageous and unoriginal statements that served as the starting point for the special services' brainstorming:

1. During his rule, Putin has increased Russia's GDP 12-fold.
2. Putin has increased Russia's gold reserves 48-fold.



FSB director Aleksandr Bortnikov (left), President Vladimir Putin, and SVR director Sergey Naryshkin; to Russian special services, a good relationship with the President is of the utmost importance.

Source: Alexei Druzhinin / AP

In 2022, the special services continued to feed the target group with primitive and hackneyed tropes that frame the president's unpopular decisions as a cunning tactic against opposing countries. Let's look at some of the new ideas added during the year:

1. Russia is the world's largest supplier of titanium and palladium, thanks to which the Russians can do without Western cars and planes.
2. Russia imposed a flight ban over its airspace in response to the West's similar actions, which is why Western countries must spend significantly more time and money to fly to Asia.
3. Russia's special operation is destroying laboratories in Ukraine where the United States, Germany, and France developed biological weapons.
4. With the mutual closure of media channels, the West ruined its opportunities to influence the Russian audience.
5. The Western countries' continued solidarity and support for Ukraine are driven by the desire to subjugate Ukraine to gain access to its grain, mineral resources, and cheap labour.

Russian special services' eagerness to invent propaganda points and disseminate them to the public often overstretches their capabilities.

CHAPTER 5

RUSSIAN INFLUENCE 54

THE CANDLE OF THE 'RUSSIAN WORLD' IS BURNING OUT

The Kremlin uses the Russian Orthodox Church (ROC) as an outpost of its struggle against Ukraine and the West.

The Russian special services are trying at all costs to preserve the structures of the ROC as a tried-and-tested cover in foreign countries.

Russian terror in Ukraine irreversibly damages the position and international influence of the ROC.

In our 2019 public threat assessment, we said that in the event of Russian aggression, the Russian Orthodox Church, one of the Kremlin's long-standing tools of influence, would not show solidarity with the victim of the attack but would side with the Kremlin. The support of the ROC leadership for Russia's military activities in Ukraine clearly demonstrates this in word and deed. In his increasingly crude anti-Ukrainian and anti-Western appeals, Patriarch Kirill (secular name Vladimir Gundyayev) expresses the church and state leaders' understanding of the "symphony" of the church and the state. In what follows, we will look at how the Kremlin and the Russian special services continue to use the networks of the ROC, which seeks to establish itself as the only orthodox church in the former territories of the Russian Empire and the Soviet Union.

Since the 1990s, the Russian special services have been using the more radical pro-Kremlin clergy and church members with links to Soviet and Russian special services to undermine Ukraine's statehood. In line with Russia's divisive policy and following in the footsteps of tsarist Russification policy, the Moscow Patriarchate, which established itself in Ukraine in the 17th century (and in Estonia and Latvia in the 18th century) in the wake of a Russian invasion, seeks to present itself as the "mother church" of Ukrainians. It claims to have the exclusive right to unite Russians, Ukrainians and Belarusians into a single "trinity", a great superpower family led by

Moscow, while disparaging the choices Ukrainians make for themselves. In tandem with other Russian propaganda channels, branches of the ROC spread anti-Ukraine propaganda in both sermons and propaganda publications in 2022, right before Russia's full-scale invasion. For example, in January, when the Kremlin needed anti-Ukraine hysteria to create a suitable backdrop for the upcoming military attack, the Estonian Orthodox Church of the Moscow Patriarchate (EOC-MP) published a special issue of its magazine *Pravoslavnyi Sobesednik* that contained slander and false claims against Ukraine and Estonia.

Clergy members recruited by or collaborating with the Russian special services have been tasked with gathering information about the moods in Ukraine, key individuals, and the location and composition of Ukrainian military units. For example, the Russian special services were particularly interested in the information collected by the ROC army chaplains, in violation of the seal of confession, about the health and morale of Ukrainian soldiers. By now, Ukraine has blocked the access of the ROC clergy to the Armed Forces of Ukraine.



ROC's public support for the war in Ukraine accelerates the disintegration of its remaining network in Ukraine.

Source: Alexey Pavlishak / Reuters

While planning military operations against Ukraine, the ROC clergy working with the Russian special services and the trustees of Russian extremists in ROC congregations provided logistical support to Russia. For example, they prepared accommodation and weapons caches for Russian units and stored propaganda materials in congregation houses and convents.

Clergy members have been tasked with gathering information about the moods in Ukraine.

Simultaneously with the Russian attack, ROC representatives curated by the Russian special services were activated. They incited anti-Ukrainian sentiments and supported the occupants near the frontline and in Russian-controlled areas. In Ukrainian-controlled territory, pro-Russian clergy often engaged in "silent resistance", cautiously justifying Russia's motives among their congregations and ambiguously passing judgement on the "fratricidal war".

ROC helped formalise the annexation of Ukrainian territory. While in 2014, Kirill, then also the patriarch of the Ukrainians, preferred to keep a low profile during the annexation of Crimea, fearing damage to the position of the Ukrainian branch of the ROC (estimated at 50 per cent of ROC congregations) after the full-scale invasion in 2022, the ROC leadership helped prepare and even anticipated the formal annexation of four regions of Ukraine by Russia. In June 2022, the Holy Synod of the Moscow Patriarchate decided to separate the territories of Crimea, Donetsk and Horlivka from its formally independent Ukrainian branch (without asking for these regions' consent) and subordinate them directly to the Moscow Patriarchate. ROC representatives participated in the ceremony to declare the territories usurped from Ukraine as part of Russia in the Kremlin on 30 September 2022. The ROC can apply a similar divide-and-rule policy elsewhere if Russian aggression creates favourable conditions for this.

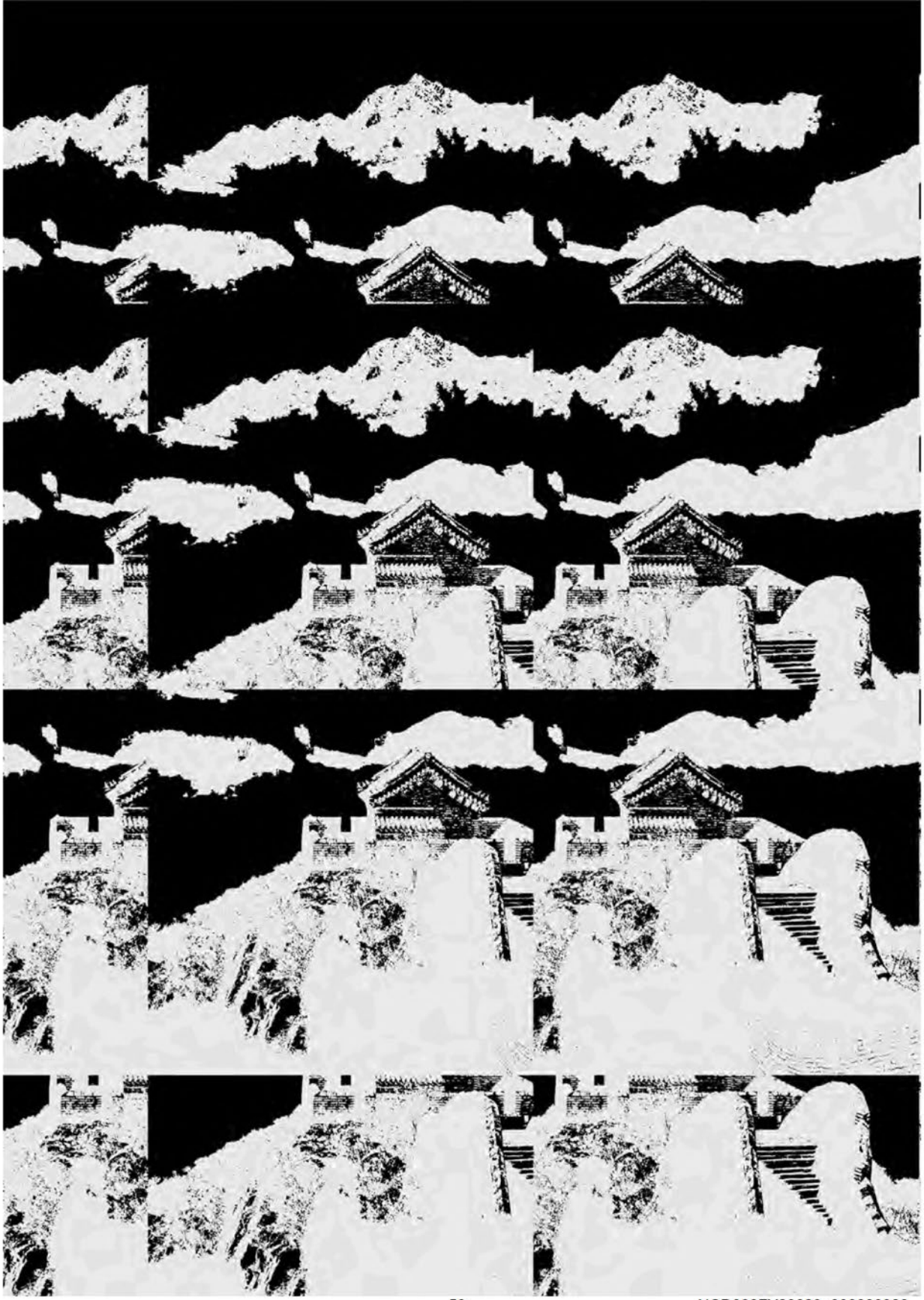
Russia's large-scale terror in Ukraine, which also destroys the ROC's Ukrainian congregations and church buildings, accelerates the disintegration of the remaining ROC network in Ukraine. Disagreements between the Putin-worshipping ROC establishment and its foreign branches have intensified. Russia's war against Kyiv, the cradle of Eastern Slavic Orthodoxy, with the help of Iranian drones and Kadyrovites preaching "Russian Jihad", is also causing increasing resentment among the ROC congregations in Russia, where hundreds of courageous clergy have publicly expressed their opposition on ethical grounds. All this puts the leaders of the ROC branches, especially those in the West, in a difficult situation: they need to remain obedient to their spiritual leader, the Kremlin puppet Patriarch Kirill, while also maintaining normal relations with the host country, which disapproves of the Russian leadership.

The leadership of the Moscow Patriarchate and its curators in the Russian government structures are aware of the ROC's difficulties abroad, especially since the Kremlin itself is undermining the position of the leaders of the ROC and its branches. Maintaining the position of the ROC in foreign countries is crucial to the long-term interests of the Russian special services, which is why the leaders of the ROC branches have been given the liberty to pretend to be a loyal local religious organisation and, if necessary, even criticise the positions of the Kremlin or ROC leadership, or simply criticise the war without clearly pointing out who is responsible. In this way, Russia seeks to create the impression that the local ROC branches are independent, diverting attention away from the fact that they are curated by Russia, which has become a pariah state.

Disagreements between the Putin-worshipping ROC establishment and its foreign branches have intensified.

Russia's aggression and the use of the ROC as a weapon against Ukraine have strengthened the international community's perception that the ROC foreign branches' independence is merely an illusion unless they completely separate themselves from the ROC. The security threat posed by the symbiosis of the Russian special services and the ROC has already called into question the future of the ROC in Latvia, where the Orthodox Church is moving towards independence, and in Lithuania.

However, Russia is trying to prevent the disintegration of the ROC's international network at all costs. In June 2022, Metropolitan Hilarion (Grigory Alfeyev), the head of the Department for External Church Relations of the Moscow Patriarchate, or the "foreign minister of the ROC", was retired, accused of numerous failures, especially his inability to prevent the independence and strengthening of the autocephalous Ukrainian Orthodox Church. Metropolitan Anthony (Anton Sevryuk), a former private secretary to Patriarch Kirill, who has experience in influence operations against the West, was appointed as the new head of the department, which has a tradition of operating as a cover for Soviet and Russian special services. Anthony's task is to save what he can of the ROC's damaged reputation in the international arena, where he tries to continue to promote the Russian regime of terror and the ROC as a bastion of "traditional values". However, it is increasingly difficult to find "useful idiots" in the West who would want to cooperate with the ROC or line up to defend it. Like other instruments of Russia's influence operations, the ROC is on the brink of an inevitably deepening crisis.



CHAPTER 6

CHINA

60

CHINA'S GLOBAL EMBRACE

The absolute power achieved by Xi Jinping at the Communist Party Congress set the tone for China's development over the next 100 years.

Chinese intelligence services plan to use the Global Security Initiative to disrupt the Western security architecture.

Xi Jinping's pledge to open China up to the world means an even more vigorous implementation of the Belt and Road Initiative.

In 2022, Xi Jinping's confirmation for a third term as general secretary of the Chinese Communist Party (CCP) was a landmark event in China's development, which Xi said will usher in the next 100 years of development in China. Xi loyalists hold an unprecedented majority in the new seven-member Standing Committee.

Health permitting, Xi Jinping is very likely to stay in office for a fourth term, continuing to lead the party, the military and the country beyond 2027, as the 20th Congress's reshuffle of the CCP leadership does not clearly point to a successor for Xi Jinping. Twenty years in power, however, would exacerbate tensions within the party and the possibility of a replay of the events of the 1970s, when Mao Zedong's autocracy completely paralysed the party and state leadership, the economy collapsed, and infighting within the party was rife.

During Xi Jinping's third term over the next five years, authoritarianism will likely deepen, and relations with the West will likely continue to deteriorate. Although a marginal part of the overall proceedings, the foreign policy section of the 20th Party Congress was very telling. The wording and context of the congressional report make it very clear that China's goal for the coming years is to build a strong community of like-minded countries opposed to the West, in line with the Cold War bloc mentality. Based on the report, China will focus particularly on developing countries and organisations such as BRICS and the Shanghai Cooperation Organisation (SCO).

China's rhetoric and worldview have clearly changed. Whereas China previously presented itself as a great power with regional ambitions, denying Western allegations of

China's global ambitions while keeping a low profile like Deng Xiaoping, it no longer hides its ambition of becoming a global superpower. At the same time, China has begun to push a vision of universal rights for humanity, constructing what the CCP's rhetoric paints as a new, more just and practicable concept of human rights. In the past, China was a firm denier of universal human rights, claiming the concept was merely a Western instrument for interfering in other countries' domestic affairs.



China's goal is to undermine and reshape the Western security architecture through the Global Security initiative.

Source: Mark Schiefelbein / AP

A major new cooperation initiative in 2022 was the Global Security Initiative (GSI), unveiled by Xi Jinping in April 2022. Chinese intelligence believes that the accession of a critical number of countries (with a focus on developing countries) to the GSI would effectively disrupt the Western security architecture. Throughout 2021, China kept talking at a very high level about the need to reshape the European security architecture considering Russia's interests. According to Chinese vice foreign minister Le Yucheng, NATO should be consigned to the ash heap of history. Such systematic and calculated efforts by China also undermine Estonia's security.

China's rhetoric and worldview have clearly changed. Previously China presented itself as a great power with regional ambitions – now China no longer hides its ambition of becoming a global superpower.

In addition to a political dimension, China's "global embrace" naturally also involves technological integration, trade and scientific cooperation in building an autonomous microcosm with like-minded states. At the CCP's 20th Congress, Xi Jinping stressed China's goal of even greater openness and becoming a technological superpower by 2035. While China's message seemingly invites the world to export its goods to China (as opposed to the protectionist US), in CCP's vocabulary, "opening up the country" means implementing the Belt and Road Initiative even more effectively. This implies an increasingly systematic construction of an autonomous Chinese microcosm.

China's foreign policy of the "new era" is increasingly confrontational with the West. Still, it is also stepping up its efforts to find and engage with like-minded individuals, associations and countries in the West. Chinese intelligence services do not necessarily seek individuals with a similar worldview. They also target high-profile critics of China who would be willing to continue their criticism while spreading the message that China cannot be ignored. This is why not only ordinary citizens but also intelligence officers are waiting for China's Covid restrictions to be relaxed so they can resume organising their ostensibly innocent platform events for recruitment purposes.

CHINA'S CALCULATIONS ON ATTACKING TAIWAN

China's changed rhetoric suggests a desire to constrict the existential space of Taiwan: Taiwan duli versus Taidu.

It is not certain that Western sanctions will deter China, as China has strong countermeasures in place.

China is very unlikely to attack Taiwan in 2023, but the likelihood will increase with time.

The Chinese Communist Party's anti-Taiwan rhetoric has recently undergone a significant change. Whereas China previously used the term *Taiwan duli* to refer to Taiwanese independence, the term used now is *Taidu*. Both mean Taiwanese independence in Chinese, but the shorter version has a broader meaning, describing not only pro-independence forces but anyone who supports building a stronger Taiwanese identity and civil society. This means that China has decidedly broadened its anti-Taiwan spectrum in order to constrict the existential space of Taiwan. The term *Taidu* was included in the revised party constitution presented at the 20th CCP Congress.

Central to the possible attack on Taiwan is Xi Jinping, who feels he personally has a historic mission to unite China by conquering Taiwan. Objectively, China has a number of factors that do not support an attack, but Xi's personal vision is very likely to override these. What factors play a role in China's calculations?

Central to the possible attack on Taiwan is Xi Jinping, who feels he personally has a historic mission to unite China by conquering Taiwan.

First – sanctions. Normally, Western sanctions in the event of an attack on Taiwan should deter China, but sanctions did not discourage it in Hong Kong or Xinjiang. Neither was China deterred by Western sanctions (some of which are still in place) during the 1989 Tiananmen massacre. While it respects the sanctions imposed on Russia, China considers them unlawful. In addition, China would impose counter-sanctions (e.g. on rare earth minerals and supply chains). Xi Jinping believes he has a sufficiently effective response to Western sanctions.



Since 2021, the relationship between Lithuania and China has deteriorated – the opening of the Taiwanese Representative Office in Vilnius alone was enough to anger China; using the name "Taiwanese" added fuel to the fire. The image here displays the name "Taiwan" at the representative office in Brussels.

Source: private collection

Another important factor is restricted access to Western markets. Given the negative outlook for China's real estate sector and the rapid increase in the debt burden, exports will be crucial to generate growth in China. At the same time, China needs to consider the potential of substitute markets. A number of Chinese initiatives with a global reach clearly indicate that China is deliberately focusing on large markets outside the Western countries to improve its ability to operate independently of the West. It is not a question of calculating whether the new markets will be able to match Western markets in terms of export volumes but whether Xi Jinping thinks they will be enough for China to survive.

The third and probably one of the most crucial factors is restricted access to Western technology and know-how. In addition to the industriousness of the Chinese people, China's technological success largely relies on access to cutting-edge Western technology. The CCP has set itself the goal of becoming a technological superpower by 2035, but it will not succeed without using Western technology and recruiting Western scientists.

The fourth factor is the unity and resilience of the West and like-minded countries against China. Western unity regarding Ukraine surprised China, but it believes this unity will crumble. Concerning Russia's aggression, China asked its businesses to assess the prospects for the Russian economy over the course of at least 12 months, which shows that China is prepared to bet on a longer time frame in anticipation of Western unity collapsing.

An attack on Taiwan would create major internal tensions in China from an economic point of view. In this context, Xi Jinping's emphatic message of unity at the 20th CCP Congress and the change in his tone of voice when he emphasised the phrase "dare to fight" (ganyu douzheng) – China must be ready for confrontation – while reading out the report is particularly noteworthy. Xi Jinping probably has at least a decade of political life left. China is very unlikely to attack Taiwan in 2023, but the likelihood will increase with time.

CHINESE-RUSSIAN RELATIONS IN THE CONTEXT OF THE WAR IN UKRAINE

The war started by Russia in Ukraine has not radically changed the relations between China and Russia. But some pre-war trends have strengthened, likely increasing the inequality in their relationship.

With China's support, Russia hopes to reduce the impact of the restrictions imposed on it due to the war, which increases Russia's economic and technological dependence on China and its preparedness to appease China on divisive issues.

Russia still plays a significant role in China's global ambitions, so it is premature to see Xi Jinping's restrained support for Putin's war as a sign of distancing from Russia.

Confrontation with the West has brought China and Russia closer in recent years. On a global scale, the war in Ukraine helps to gauge the degree of polarisation in the relations between democracies and authoritarian regimes.

Russia's claims that the West, led by the United States, initiated the aggression in Ukraine and that Russia's attack on Ukraine was forced self-defence are compatible with China's pragmatic goals arising from its increasing confrontation with the US. Since the beginning of the war, the Chinese media has clearly sided with Russia, spreading Russian narratives and calling the US the real culprit of the war while painting Ukraine and the countries that support it, including the Baltic states, as puppets of the US. When covering the war in Ukraine, the Chinese media often uses propaganda produced in Russia – this also points to the fact that in terms of values, Russia is much closer to China than one might expect based on their diplomatic cooperation.

Aspiring to become a world leader in counterbalancing Western democracy and reduce its vulnerability to economic restrictions, China is intensively cultivating and

strengthening a community of like-minded countries. Russia plays an important role in China's efforts to reach this goal, which should not be underestimated by anyone wanting to see signs of deteriorating relations between the two states. From a political point of view, Russia is almost the only partner for China with a considerable diplomatic position and the ability to exert significant influence on international relations and the balance of power, including in international organisations.

Given China's global ambitions, Russia is much more useful as a friend than an enemy.

Given China's global ambitions, Russia is much more useful as a friend than an enemy, and it is not insignificant that the contrast with an aggressive and unpredictable Russia allows China to maintain the image of a fair and peaceful power while pursuing the same goals as Russia. This may be the reason behind some inconsistencies in China's official statements about the war in Ukraine. For example, last September, Li Zhanshu, the then-chairman of the CCP Politburo Standing Committee, expressed his full support for Russia's military actions in Ukraine when he visited Moscow. However, Xi Jinping, the party's general secretary and head of state, remained quite tongue-tied when he met with Vladimir Putin just a few days later, expressing only China's readiness to cooperate with Russia for world peace and stability.

From an economic point of view, Russia is an energy supplier to China and, thanks to a land connection, would retain this role even if sea routes from other countries were blocked. Supplying energy to China reduces the impact of war-related sanctions on Russia. However, China always puts its own interests first when carrying out its plans, and although the outbreak of the war in Ukraine was probably not good news for China, it tried to quickly adapt and benefit from it, sometimes at the expense of its alleged partner, Russia.

China has a clear advantage in its relations with Russia. Although the two countries agree and work together on many issues, the Russian leadership was concerned about the growing asymmetry even before the start of the war. Russia is most concerned about foreign policy, where China's vigorous activity has begun to undermine Russia's position in international organisations and in regions that the latter considers part of its sphere of influence.

The Shanghai Cooperation Organisation (SCO) summit held in Samarkand in September 2022 vividly demonstrated that the balance of power in Central Asia has begun to shift in China's favour due to the impact of the Covid pandemic and the war. Ceding positions to China in Central Asia, which Russia considers its traditional sphere of influence, is difficult for Russia, especially if it implies an increased Chinese military presence in the region. While China knows Russia may not like the strengthening of China's relations with countries in Central Asia, its goal is neither to please nor to challenge Russia but to promote its own interests.

China and Russia will continue to compete for influence in non-Western organisations such as the SCO and BRICS. The two states are united by their desire to strengthen anti-Western sentiments in the member states of these organisations and involve them in the plan to reduce the dominance of the US dollar. At the same time, Russia is anxiously watching China's bilateral relations with the countries of these organisations and making diplomatic efforts to counter trends that could undermine its position.



China's goal is neither to please nor to challenge Russia but to promote its own interests.

Source: Sergei Bobylev / AP

Technologically lagging behind the West, Russia hopes to improve cooperation with China in the near future to help China achieve independence as a technology producer, thereby reducing Russia's own dependence on Western technology. In the long run, this carries the risk of becoming dependent on Chinese technology.

China was surprised by Western unity and determination in imposing large-scale sanctions against Russia. From the beginning, China has closely monitored the war in Ukraine and its impact on the global balance of power. On the one hand, this helps adapt to rapid changes and new challenges. On the other hand, learning from Russia's mistakes, China can make better choices and pick a more effective strategy if its confrontation with the West becomes significantly sharper and it finds itself in international isolation similar to Russia – for example, should China begin military aggression against Taiwan.

In the near future, China will continue to put its interests first and behave pragmatically in relations with Russia; it will express support for Russia in its rhetoric and use Russian war narratives to undermine transatlantic cooperation. At the same time, China will likely refrain from endorsing the war, violating secondary sanctions or recognising the occupied territories in Ukraine as part of Russia. It will also likely avoid providing military assistance at the government level. However, this does not preclude the supply of goods with dual and military purposes to Russia by private businesses.

China will very likely continue to use its leverage to force Russia to support its agenda. The more Russia is prepared to give in to China to mitigate the impact of Western sanctions, the less leeway it will have for independent decisions where China's goals differ from its own or are detrimental to them.

ISSN: 2461-4459 (print)
ISSN: 2613-3288 (online)
Cover photo: Photographer Priit Mürk/ ERR
Translation by Margus Elings, Refiner Translations OÜ
Editing by Scott Abel, Tekstikoda OÜ

NCD008FY23023_000000388

EXECUTIVE SUMMARY

1. The Ukrainians' will to defend, the capabilities of their Armed Forces, and Western unity in supporting Ukraine surprised the Kremlin. Despite this, Russia's strategic goal remains the same: subjugating Ukraine and changing the European security architecture. Read more in chapters 1.1, 2.1.

2. Russia believes that time is on its side. To keep the war machine going, Russia is ready raise the stakes. Russia seems to believe it can "bomb" Ukraine to the negotiating table. Read more in chapter 1.1.

3. Russia's belligerence has significantly increased the security risks for Estonia, and the large-scale exercise Zapad 23 may further strain the situation in the Baltic Sea region. Russia still has enough strength to exert credible military pressure in our region. Read more in chapter 1.2.

4. Russia supports its military efforts in Ukraine by using cyber tools against Ukraine and the countries that support it. Its activities in cyberspace have not yielded the results Russia had hoped for, but we must remain vigilant. Read more in chapter 1.3.

5. The Russian special services officers hide behind various "covers". A tried-and-tested cover organisation used abroad is the Russian Orthodox Church, which the Kremlin also operates as an instrument of influence against Ukraine and the West. Read more in chapters 4, 5.

6. Belarus has provided logistical and material support to Russia in the war against Ukraine, but the Belarusian Armed Forces have not yet intervened in the military operations in Ukraine and do not wish to do so in the future. Read more in chapter 1.4.

7. Russia is moving towards a total dictatorship. The prospects for the current regime collapsing and the country democratising are slim despite the problems caused by the war and Western sanctions. On the contrary, an even more radical faction is rising to the fore in Russia's ruling elite. Read more in chapter 3.1.

8. In foreign policy, Russia has its stakes on creating a geopolitical coalition of authoritarian regimes opposed to the West who share a mistrust of Western policies and values. Diplomatic resources are being diverted from the West to other regions. Read more in chapter 2.1.

9. Russia's military credibility in former Soviet territories has weakened because Russia has failed to provide the security guarantees promised within the CSTO framework, and its Armed Forces have been unsuccessful in Ukraine. In Africa, however, Russia sees its best opportunities precisely in the field of security. Read more in chapters 2.2, 2.3.

10. Under Xi Jinping, China is moving towards deepening authoritarianism and no longer hides its ambition to become a global superpower. China's efforts to build a community of like-minded countries opposed to the West under the banner of the Global Security Initiative – which would also include Russia – undermines Estonia's security. Read more in chapter 6.

NCD008FY23023_000000388

Intelligence Update

14 February 2023

Munich Security Conference

Chinese mobile masts loom over the Munich Security Conference: Analysis from journalists at the Politico suggests that several locations in Munich, including the venue for the conference (Bayerischer Hof), host 4G/5G antenna masts with Huawei signals processing equipment. The political dissonance is interesting and provides insight into German domestic policy.

- **U.S. Commentary:** When asked about Huawei's presence in Munich, Mike Gallagher, a Republican and Chairman of the U.S. House select committee on China, said POLITICO's findings were "troubling" and "should concern every individual attending the conference." The chair of the U.S. Senate intelligence committee, Mark Warner, a Democrat who's attending the conference, said it was "a timely reminder that we must continue to work with like-minded allies to promote secure and competitively priced alternatives to Huawei equipment." U.S. Senate intelligence committee Vice Chair Marco Rubio (Republican, Florida) said U.S. diplomats "should be aware of the risks and take necessary precautions."

- **German telecommunication infrastructure**: The findings are in line with recent reports on Germany's telecoms infrastructure. Europe's largest economy is a stronghold for Huawei in the West. A report by boutique telecoms intelligence firm Strand Consult estimated that ***Germany relies on Chinese technology for 59 percent of its ongoing 5G network deployment***. The country already had a massive reliance on Chinese equipment in its 4G network, where Strand estimated Huawei accounts for 57 percent. "If you look at the percentage of Chinese equipment in Germany, you could say it is the most unsafe country in Europe," said John Strand, founder of Strand Consult. ***"Welcome to the Munich Security Conference: We can't guarantee your security,"*** he quipped.

International Security and Estonia 2023: Estonian Foreign Intelligence Service published the eighth edition of their annual report on 8 February 2023. Land war in Europe is the focus of the assessment with some light touches on China. The key takeaways in the executive summary are very good and they are included below to support dialogues, as needed.

- The Ukrainians' will to defend, the capabilities of their Armed Forces, and Western unity in supporting Ukraine surprised the Kremlin. Despite this, ***Russia's strategic goal remains the same: subjugating Ukraine and changing the European security architecture***.

- Russia believes that time is on its side. To keep the war machine going, Russia is ready raise the stakes. Russia seems to believe it can "bomb" Ukraine to the negotiating table.

- Russia's belligerence has significantly increased the security risks for Estonia, and the large-scale exercise Zapad 23 may further strain the situation in the Baltic Sea region. Russia still has enough strength to exert credible military pressure in our region.

- Russia supports its military efforts in Ukraine by using cyber tools against Ukraine and the countries that support it. ***Its activities in cyberspace have not yielded the results Russia had hoped for, but we must remain vigilant***.

- The Russian special services officers hide behind various "covers". A tried-and-tested cover organization used abroad is the Russian Orthodox Church, which the Kremlin also operates as an instrument of influence against Ukraine and the West.

- Belarus has provided logistical and material support to Russia in the war against Ukraine, but the Belarusian Armed Forces have not yet intervened in the military operations in Ukraine and do not wish to do so in the future.

- Russia is moving towards a total dictatorship. The prospects for the current regime collapsing and the country democratizing are slim despite the problems caused by the war and Western sanctions. On the contrary, ***an even more radical faction is rising to the fore in Russia's ruling elite***.

- In foreign policy, Russia has its stakes on creating a geopolitical coalition of authoritarian regimes opposed to the West who share a mistrust of Western policies and values. Diplomatic resources are being diverted from the West to other regions.

- Russia's military credibility in former Soviet territories has weakened because Russia has failed to provide the security guarantees promised within the CSTO framework, and its Armed Forces have been unsuccessful in Ukraine***. In Africa, however, Russia sees its best opportunities precisely in the field of security***.

- Under Xi Jinping, China is moving towards deepening authoritarianism and no longer hides its ambition to become a global superpower. ***China's efforts to build a community of like-minded countries opposed to the West under the banner of the Global Security Initiative – which would also include Russia – undermines Estonia's security***.

War in Ukraine

New Russian offensive underway in Ukraine: Eastern Ukrainian city of Bakhmut is facing heavy artillery fire as NATO corroborates local reporting that a major new Russian offensive has begun, days before the first anniversary of Moscow's invasion. "There is not a single square metre in Bakhmut that is safe or that is not in range of enemy fire or drones," Pavlo Kyrylenko, governor of the Donetsk region, told the Ukrainian national broadcaster late on Monday. (Reuters)

Russia's War in Ukraine, Military and Intelligence Aspects: The Congressional Research Service just updated a very robust temporal analysis of the war in Ukraine, which should serve the ONCD delegation with a sound, authoritative reference, with timelines, for what has happened so far. More interestingly, Carnegie's analysis was sourced for the single paragraph of the cyber assessment (yes, cyber made it, but just barely) in the context of poor military coordination during the initial invasion. ***Please note, ONCD does have talking points for Russia's use of cyber in Ukraine.***

- Russia's cyber operations were largely ineffective during the initial invasion, surprising many observers. Some analysts suggest Russian cyber performance possibly indicates the limitations of cyber operations in a kinetic conflict as well as structural limitations of cyber operations in the Russian military

- **Outlook for 2023**: Ultimately, the war remains an artillery battle. Both sides are consuming large quantities of ammunition. Continued supplies will be a key variable in the conflict. While UAF is receiving additional tanks and armored personnel carries to support offensive operations, ***observers remain concerned over the ability of the UAF to maintain and support the various equipment variants it is receiving, each with different maintenance, ammunition, and training requirements***

- **Issues for Congress:** The key takeaways for the legislature include providing further funds (military and economic assistance) to support Ukraine, oversight and accountability for the security assistance, investigations of Russian war crimes, and sanctioning malign Russian actors such as the Wagner group.

Starlink's revised support for Ukraine: SpaceX restored connectivity to Ukraine's disrupted networks in the war's earliest days, and did so to considerable acclaim. The company is now interfering with services to its Ukrainian customer, saying that military uses are outside the scope of what it agreed to.

- CNN reports that SpaceX president explained, "There are things that we can do to limit their ability to do that. There are things that we can do, and have done." Ukraine used the technology too creatively, she said. "It was never intended to be weaponized. However, Ukrainians have leveraged it in ways that were unintentional and not part of any agreement."

- But as Defense One points out, these statements sound like pious malarkey: "But Gwynne Shotwell's explanation is at odds with Starlink's role in recent U.S. Army modernization experiments that seek to fire on targets more quickly." Any loss of Starlink support from SpaceX may be offset by direct targeting information from the US military. The Washington Post reports that US forces provide targeting assistance for HIMARS and other US-supplied weapons: "A senior U.S. official — who, like others, spoke on the condition of anonymity because of the sensitivity of the issue — acknowledged the key American role in the campaign and said the targeting assistance served to ensure accuracy and conserve limited stores of ammunition for maximum effectiveness. The official said Ukraine does not seek approval from the United States on what to strike and routinely targets Russian forces on their own with other weapons. The United States provides coordinates and precise targeting information solely in an advisory role, the official said."

Europe Cyber Policy and Issues

Moldovan president warns of Russian plot to topple leadership: Moldova's president accused Russia on Monday of planning to use foreign saboteurs to bring down her tiny country's leadership, stop it joining the European Union and use it in the war against Ukraine. She said the plan involved citizens of Russia, Montenegro, Belarus and Serbia entering Moldova to try to spark protests in an attempt to "change the legitimate government to an illegal government controlled by the Russian Federation." President Maia Sandu made her comments after Ukrainian President Volodymyr Zelenskiy said last week his country had uncovered a Russian intelligence plan "for the destruction of Moldova", and days later the country's government resigned.

Russian cyberattacks aimed at 'destabilizing' Moldova: In an interview with Euronews on Tuesday, Moldovan Prime Minister Natalia Gavriliță accused Russia of trying to destabilize the country by sponsoring