17 April 2025
View the online version ›

GSIS® HAMBURG
22-23 October 2025
Global Security and Innovation Summit

organised by Hamburg Messe + Congress IISS

Monthly Executive Briefing

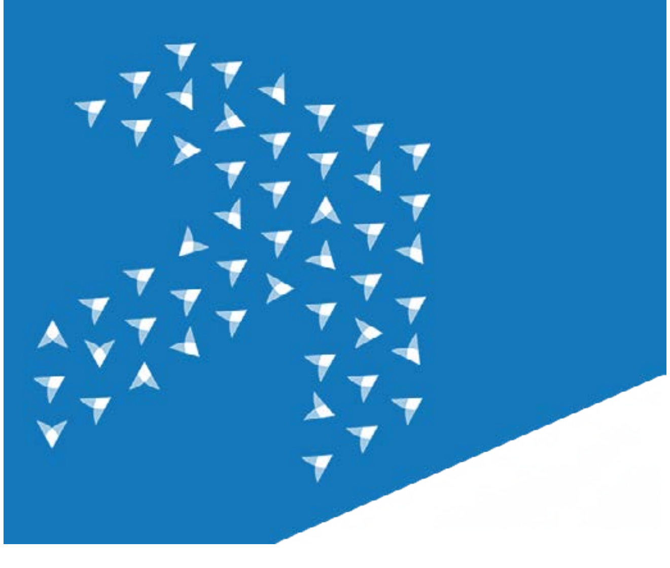
Russian threats in and through cyberspace

GSIS® HAMBURG
22-23 October 2025
Global Security and Innovation·Summit

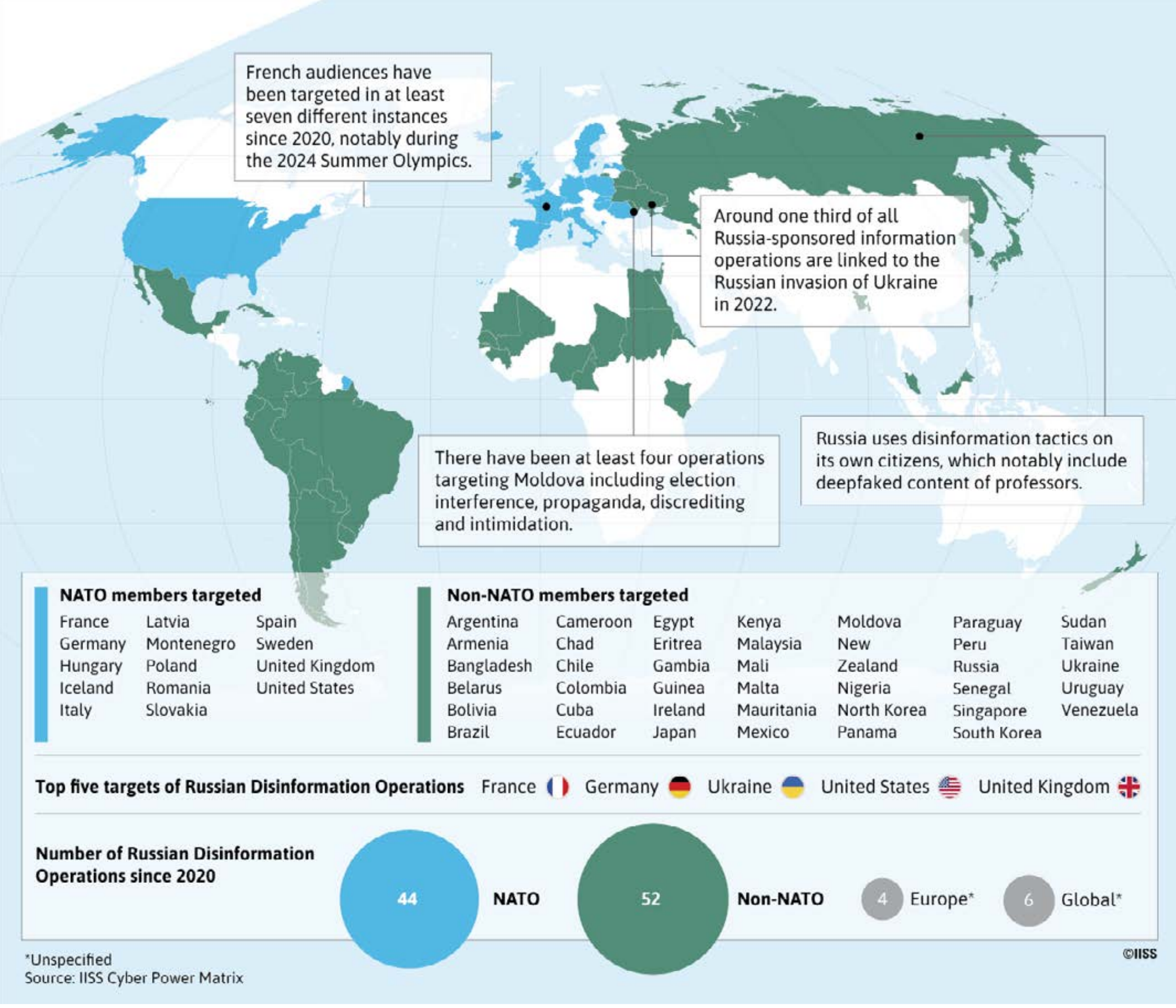
Russia has escalated its cyber and influence operations, and sabotage of digital infrastructure, exerting asymmetric pressure on governments and businesses alike.

- Russia's escalating influence efforts combine low- and high-tech methods and its networks are highly adaptive – a robust and agile whole-of-society defence strategy is critical for cognitive resilience.
- Russia has intensified cyber attacks against entities across NATO disrupting public services, critical infrastructure, and extorting organisations to fund its invasion – partners need to urgently collaborate to collectively increase cyber resilience across the board.
- Sabotage of undersea cables threatens business continuity and increases supply chain risks – NATO, partners and industry need to strengthen infrastructure protection, including advanced surveillance technologies, to mitigate growing economic and security risks.

Join industry leaders, policymakers, and security experts at the Global Security and Innovation Summit to explore solutions, strengthen partnerships, and shape the future of critical infrastructure security.



Selected Russian Disinformation Operations since 2020



French audiences have been targeted in at least seven different instances since 2020, notably during the 2024 Summer Olympics.

Around one third of all Russia-sponsored information operations are linked to the Russian invasion of Ukraine in 2022.

There have been at least four operations targeting Moldova including election interference, propaganda, discrediting and intimidation.

Russia uses disinformation tactics on its own citizens, which notably include deepfaked content of professors.

NATO members targeted

France
Germany
Hungary
Iceland
Italy
Latvia
Montenegro
Poland
Romania
Slovakia
Spain
Sweden
United Kingdom
United States

Non-NATO members targeted

Argentina
Armenia
Bangladesh
Belarus
Bolivia
Brazil
Cameroon
Chad
Chile
Colombia
Cuba
Ecuador
Egypt
Eritrea
Gambia
Guinea
Ireland
Japan
Kenya
Malaysia
Mali
Malta
Mauritania
Mexico
Moldova
New Zealand
Nigeria
North Korea
Panama
Paraguay
Peru
Russia
Senegal
Singapore
South Korea
Sudan
Taiwan
Ukraine
Uruguay
Venezuela

Top five targets of Russian Disinformation Operations France Germany Ukraine United States United Kingdom

Number of Russian Disinformation Operations since 2020

NATO	44
Non-NATO	52
Europe*	4
Global*	6

*Unspecified
Source: IISS Cyber Power Matrix

©IISS

8,000 MORE THAN US$338,000 WAS SPENT ON 8,000 FACEBOOK ADVERTS AS PART OF A RUSSIAN INFORMATION OPERATION TARGETING FRANCE, GERMANY, POLAND AND ITALY BETWEEN AUGUST 2023 AND OCTOBER 2024.

WYSOKIE CENY ENERGII TO TEŻ JEGO BROŃ
PKEE
WWW.WALCZYMY-O-NIEZALEZNOSC.PL

Chaos via disinformation

Russia has doubled down on efforts to influence global public opinion utilising a spectrum of tools from trolls and high-volume spam, to counterfeit documents, chatbots and deepfake technologies. In addition, Moscow has cultivated a network of proxy influencers in target audiences to infiltrate information channels and influence public opinion worldwide. Russia-linked actors masquerade as fact checking platforms, spoof existing news sites (e.g. Guardian, Bild, RBC Ukraine) as well as government websites (including NATO). The false narratives have focused on undermining the integrity of elections, weakening Western support for Ukraine, depicting Ukraine as a failed and corrupt neo-Nazi state, spreading Kremlin propaganda about the war, and targeting citizens in Germany, Italy, France, Latvia and the UK threatening that sanctions against Russia will ruin their lives. While states have sanctioned these actors, Russia's disinformation continues and Moscow has not taken any steps to prevent these operations from proliferating. Despite sanctions and takedowns, Russia is a sophisticated disinformation actor whose networks and methods continuously adapt. Allies need to be similarly agile and innovative, using technology defence strategy in partnership with industry. Failure to do so risks ceding the information advantage to adversaries.

> *"To the defence industry I say: You need to do everything you can to keep us safe. There's money on the table, and it will only increase. So dare to innovate and take risks! Come up with solutions to the swarms of drones and other new war tactics. Put in the extra shifts and new production lines!"*
>
> Mark Rutte, NATO Secretary-General

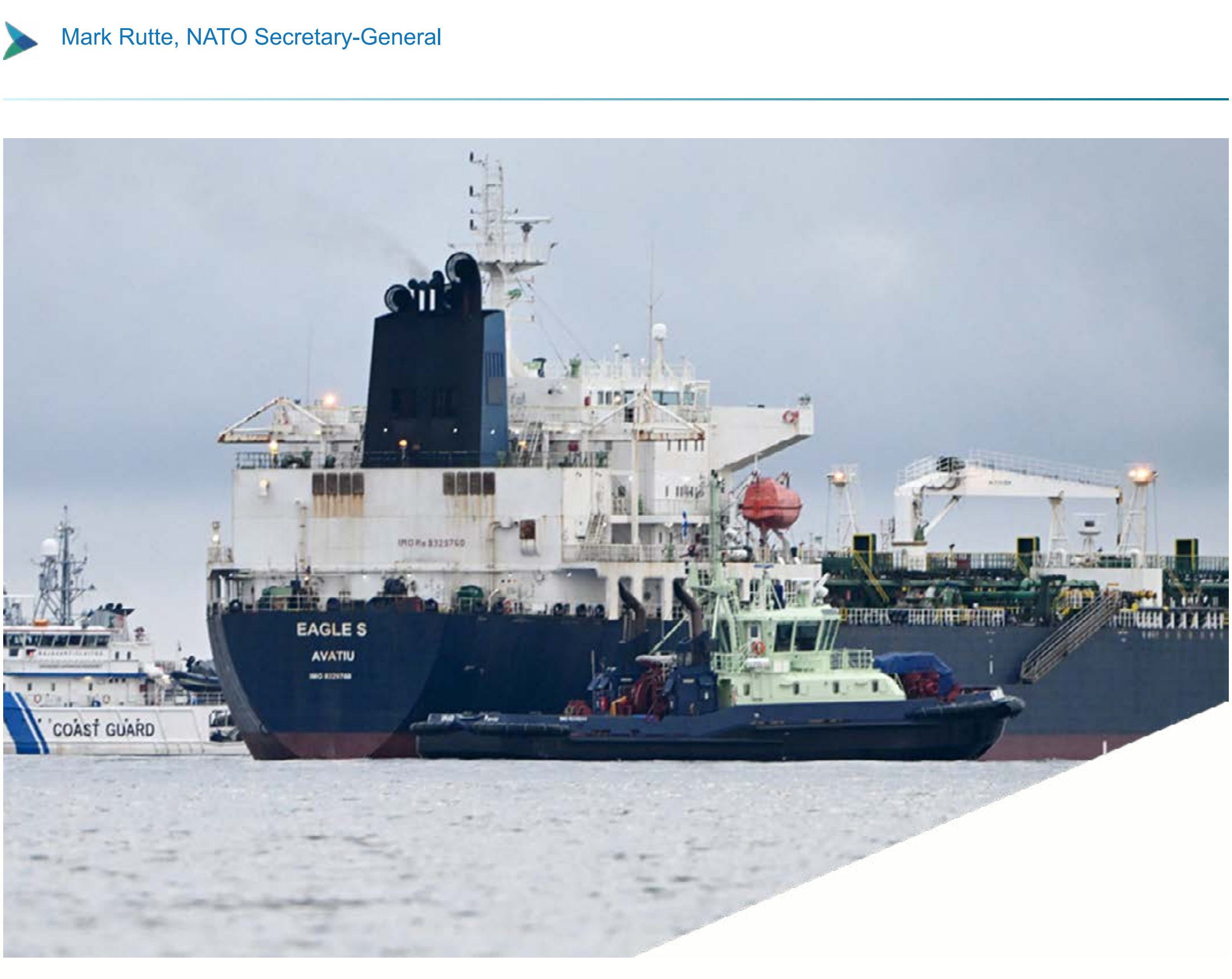
Disruptive and destructive cyber operations

Russia has expanded its attacks against Kyiv and its allies. Since July 2022, more than a third of all of Russia's cyber operations are directed against organisations within NATO member states. Large scale cyber operations aimed at disrupting government websites, and subsequently public services as well as banks and other industries, have been used to discourage support for Ukraine. Destructive malware has affected thousands of organisations across Europe, including the operation targeting Viasat's satellite network in the early hours of the 2022 invasion of Ukraine, disrupting military communications and causing 5,800 wind turbines in Germany to malfunction. Kremlin-linked criminal entities have used ransomware to disrupt critical services and extort victims, including Poland's transportation and logistics sector. In 2023, Russian ransomware gangs accounted for an estimated 70% of all ransom proceeds in excess of US$500 million. Russia has turned a blind-eye to these criminal groups with reports that some of these proceeds have been used to procure military equipment for Russia. As AI developments progress, Russian threat actors are working to integrate generative AI into their attacks. With the United States shifting its posture on Russia, it is imperative that national governments and industry move to develop and deploy innovative new technologies, including utilising AI for defence through deepened public-private partnerships.

70% RUSSIAN CYBER INCIDENTS TARGETING UKRAINE SURGED BY NEARLY 70% in 2024

75% 75% OF RUSSIAN CYBER OPERATIONS BETWEEN 2023–24 TARGETED UKRAINE OR A NATO MEMBER STATE

> *"To our governments I say: give our industries the big orders and long-term contracts they need to rapidly produce more and better capabilities. Buying only big-ticket items that are delivered too late will not keep us safe… [we need] modern capabilities that use the most advanced technologies. And we need them now."*
>
> Mark Rutte, NATO Secretary-General



Sabotage of subsea infrastructure

In the last six months, Russia has been associated with the sabotage of cables linking Lithuania and Sweden, Finland and Germany, and also Finland and Estonia. Finnish authorities discovered an almost 62-mile drag mark linked to the Eagle S anchor. Eagle S is considered part of Russia's shadow fleet used to illegally circumvent sanctions and also to conduct espionage and sabotage cables and oil pipelines. While direct attribution remains challenging due to the nature of vessel ownership, the pattern of incidents aligns with Russia's broader strategy of asymmetric warfare – using infrastructure attacks to enhance tensions, intimidate and sow economic uncertainty. In the face of the deteriorating security situation, NATO, partners and industry have intensified coordination. In January, NATO announced the deployment of 'Baltic Sentry', a military activity to enhance maritime presence in priority areas including more ships, maritime aircraft patrols, submarines, satellites and surveillance drones. In addition, the Alliance agreed to deploy new technologies to enhance surveillance and deterrence.

1.3 MILLION KILOMETRES 1.3M KILOMETRES OF UNDERSEA CABLES SECURE 95% OF INTERNET TRAFFIC

US$10 TRILLION THESE CABLES GUARANTEE US$10 TRILLION WORTH OF FINANCIAL TRANSACTIONS PER DAY EVERY DAY

GSIS® organised by: Hamburg Messe + Congress IISS

To stay ahead of emerging threats and insights follow GSIS on LinkedIn

CONTACT US

Hamburg Messe und Congress GmbH · Messeplatz 1 · 20357 Hamburg · Germany
Phone +49 40 3569-0 · Fax +49 40 3569-2203 · info@gsis-hamburg.com ·
www.gsis-hamburg.com

Follow us:

Management Board: Uwe Fischer (CEO), Heiko M. Stutzinger (CEO)
Hamburg Municipal Court, Reg. No. HRB 12 054
VAT No. DE811214125

Hamburg Messe + Congress