sps
A Concentric Company

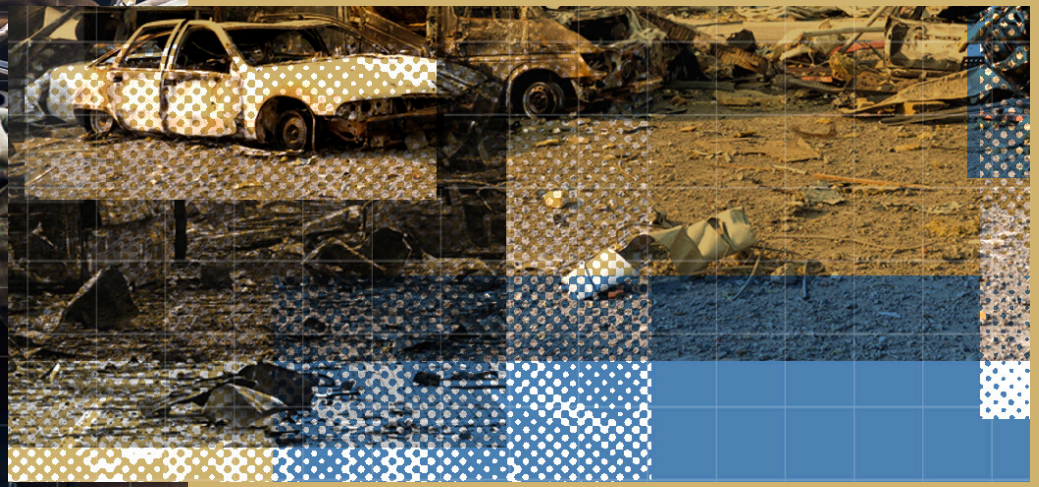
Global Insights Report

Your reliable source of intelligence for Kidnap, Ransom, Extortion and Piracy around the world

Piracy, Cyber, Ukraine

September 2025

www.sps-global.com



sps
A Concentric Company

APAC
Asia Pacific

Piracy Singapore Strait

96 Incidents

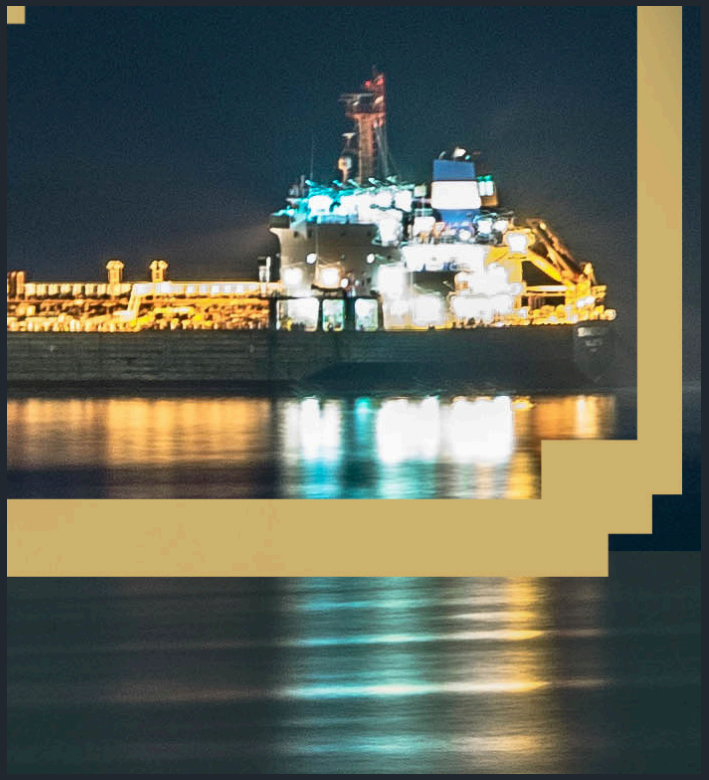
From January to August 2025, there have been 96 incidents of piracy or armed robbery at sea (ARAS) in the Singapore Strait.

Bulk Carriers

On July 1, three bulk carriers were targeted in a three mile radius in less than three hours. One of the crews reported the criminals being armed with a firearm.

Night Raids

Over 90 percent of incidents in 2025 occurred during night time hours.

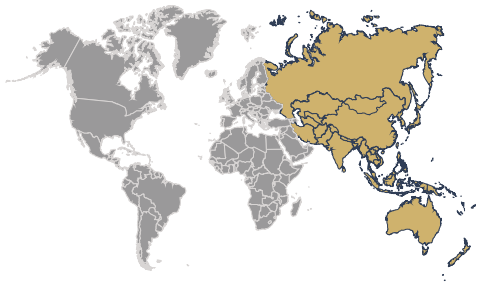


Piracy and robbery in the Singapore Strait remain an endemic issue. Indonesian-based criminal groups continue to conduct targeted boardings of commercial vessels in an area with multi-jurisdictional waters, exploiting security gaps around the eastbound lane TSS, Singapore Strait. We assess these groups, tied to broader criminal networks, are emboldened by minimal law enforcement operations and economic strain. The lack of law enforcement action has resulted in further risk to crews as violence against crew members increases.

Global Insights Report
September 2025

APAC

Asia Pacific



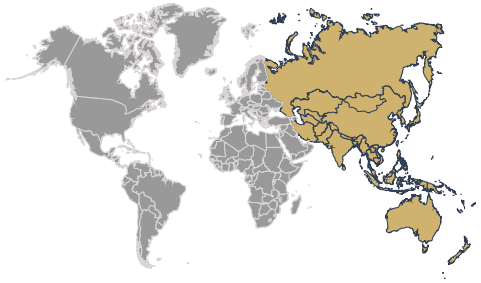
Piracy – Singapore Strait

Piracy and robbery in the Singapore Strait remains an endemic threat to commercial shipping. While the incidents typically involve theft of spares and stores, crews have been restrained and assaulted by criminals in recent incidents. The number of attacks increased in 2025. Between January to June, 80 incidents were reported in the Singapore Strait, accounting for 84 percent of all incidents of piracy and robbery in Asia. Comparatively, from January to June 2024, there were only a reported 21 incidents in the Singapore Strait, exemplifying the increase in attacks.

Global Insights Report
September 2025

APAC

Asia Pacific



Piracy – Singapore Strait

Most incidents involved the targeting of bulk carriers and tankers transiting the eastbound lane the Traffic Separation Scheme (TSS) Singapore Strait, particularly around the Philip channel.

- Criminals frequently operate in small groups using wooden boats, and board at night when vessels reduce speed to navigate congested waters.

- Crews reported either firearm-like objects, or bladed/blunt weapons used by criminals in 53 percent of incidents.

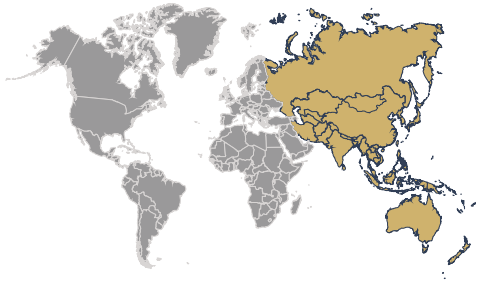
- In at least six incidents crew members were physically tied up or restrained, and in most cases the crew was physically threatened, suggesting a gradual escalation in aggressiveness in ongoing incidents.

Global Insights Report

September 2025

APAC

Asia Pacific



Piracy – Singapore Strait

Regional patrols by Indonesian, Singaporean, and Malaysian authorities including frameworks such as the Malacca Straits Patrols, have reduced some risks, but the tripartite arrangement does not fully cover every area of jurisdiction.

Criminals exploit short patrol response times, predictable vessel routing, and the chokepoint geography of the TSS to rob ships.

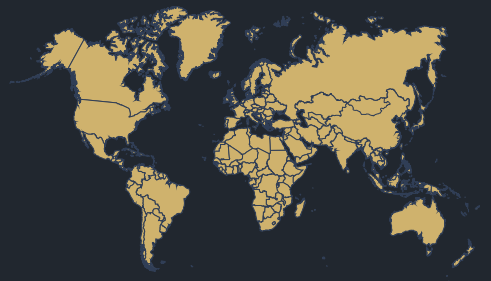
We assess without additional law enforcement patrols, opportunistic boardings, robberies, and assaults on crew will likely persist at elevated levels, sustaining a model which disproportionately disrupts commercial shipping through one of the world's busiest chokepoints.

Global Insights Report

September 2025

sps
A Concentric Company

Cyber



Global Insights Report
September 2025

Cyber

Rise of Deepfake Attacks on Executives and Corporations

Deepfake Attacks

Deepfake attacks on executives are on the rise, with 51 percent of security professionals reporting incidents in 2025 (up from 43 percent in 2023) as cheaper artificial intelligence (AI) tools and poor personal cybersecurity protocols fuel impersonations targeting business leaders.

Jaguar Land Rover

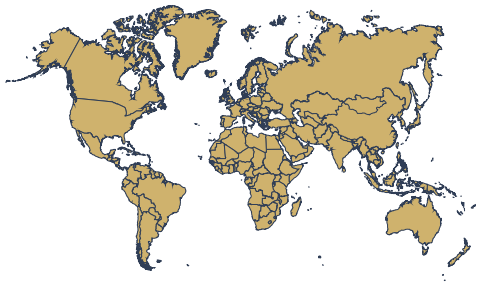
British automotive manufacturer, Jaguar Land Rover, was recently targeted by a major cyberattack, severely disrupting global operations.

Cyber-Espionage

The FBI published a report on 27 August showing a vast Chinese-sponsored cyber-espionage operation affecting around 200 U.S. organizations and victims in 80 countries.

We assess cyber threat risks will remain elevated for corporations and high-net-worth individuals as executives and businesses face growing risks of extortion, financial theft, and reputational harm. State actors, including Russia and China, further complicate the landscape by targeting sectors critical to both national security and private enterprise.

Cyber

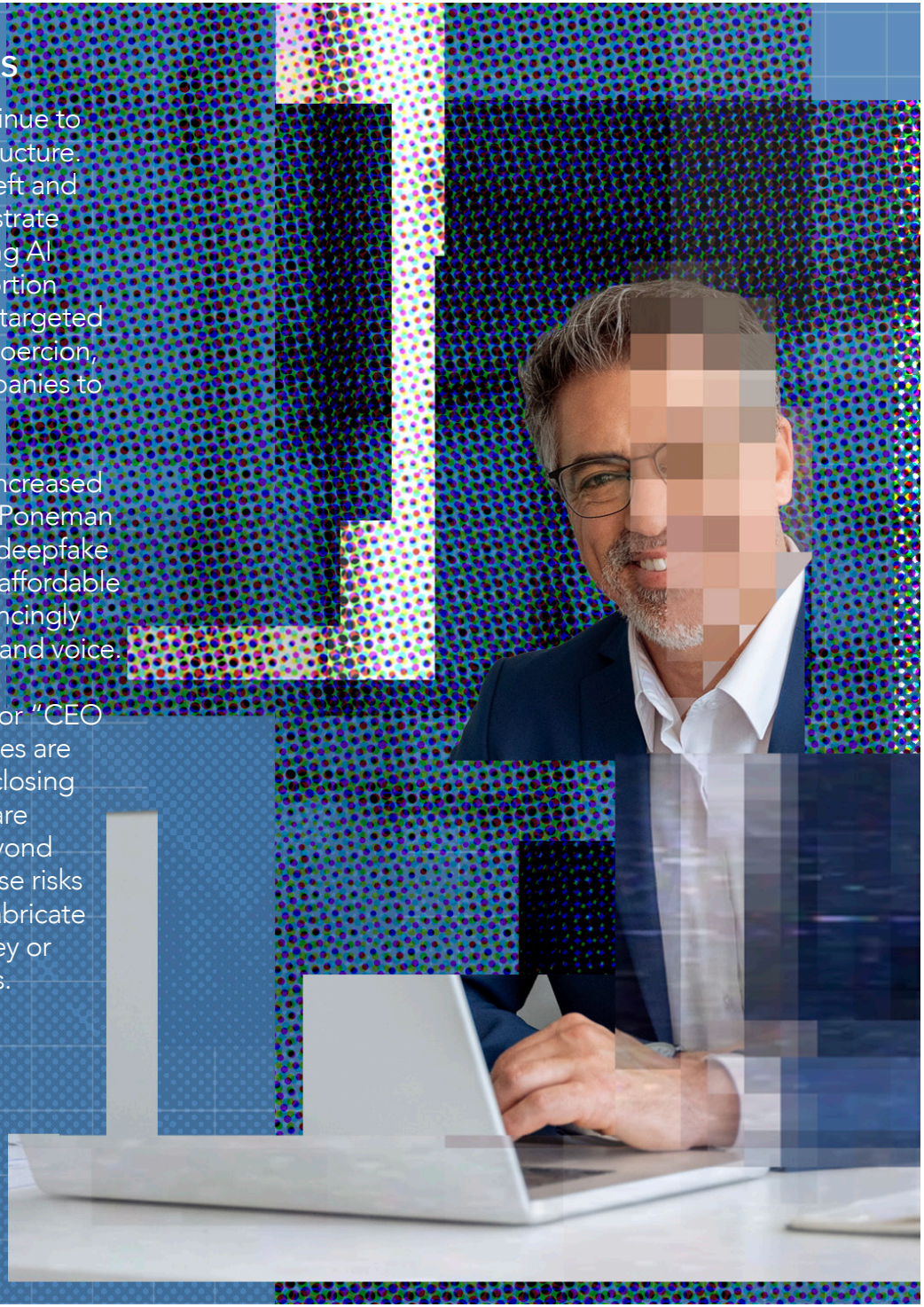


Rise of Deepfake Attacks

Cybercrime and malicious activity continue to threaten businesses and critical infrastructure. While attacks have focused on data theft and financial gain, recent incidents demonstrate a broader scope. New tactics leveraging AI and deepfakes are expanding the extortion landscape. Executives are increasingly targeted not only for financial gain but also for coercion, reputational harm, or to pressure companies to comply with broader demands.

- The number of cyber incidents has increased in 2025. The latest findings from the Poneman Institute highlighted the increase of deepfake attacks on executives and illustrates affordable AI tools now allow criminals to convincingly impersonate senior leaders in video and voice.

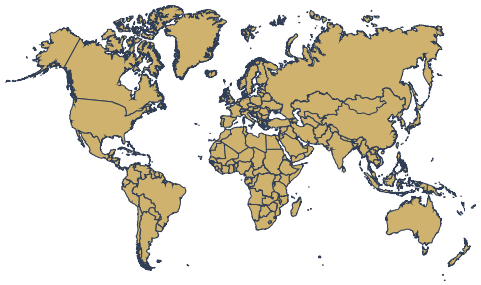
- These tactics have been deployed for "CEO fraud" operations, in which employees are tricked into transferring funds or disclosing sensitive data under the belief they are following legitimate instructions. Beyond financial theft, such methods also raise risks of blackmail, with criminals able to fabricate compromising media to extort money or concessions from high-profile figures.



Global Insights Report

September 2025

Cyber



Rise of Deepfake Attacks

In addition to AI-driven concerns, ransomware groups remain highly active. Increasingly, threat actors adopt a double extortion model, stealing sensitive data before encrypting systems, then threatening to leak information unless a ransom is paid.

- The ransomware attack on Ireland's K Club resort in June demonstrated this trend, as attackers exfiltrated sensitive data, encrypted the resort's IT systems, and subsequently leaked some of the stolen files on the darknet.

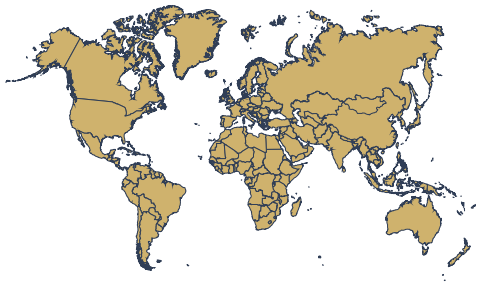
- The SafePay ransomware group which was responsible for the attack, typically demands large Bitcoin payments and threatens data leaks to apply pressure. The group is an emerging but sophisticated threat actor which began attacks in late 2024. By the first quarter of 2025, it claimed over 200 victims across various sectors, including manufacturing, healthcare, and education.

- In addition, the recent cyberattack breach on JLR paralyzed IT systems across core U.K. plants, as well as overseas facilities. It has been suggested that the company is losing around £5 million a day as the disruption continues, with the recovery process expected to take weeks, if not months. The National Cyber Security Centre has pointed out that sensitive data has been seen or stolen, signaling both the scale and sensitivity of the breach.

Global Insights Report

September 2025

Cyber



Rise of Deepfake Attacks

Cyber operations by state actors are also a persistent concern. State threats are often framed in a geopolitical context, however, the impacts can affect corporate organisations. State actors, including Russia and China, have targeted logistics, telecoms, financial services, and energy sectors, which are crucial for global business.

- In May 2025, the FBI issued a warning over the infiltration of multiple telecommunication companies by a Chinese-linked advanced persistent threat (APT), Salt Typhoon, demonstrating how espionage campaigns now compromise private companies to siphon data, monitor communications, and disrupt supply chains, even when the primary targets are related to national security.

- Looking ahead, we assess cybercrime and state-sponsored activity are expected to intensify in scale and sophistication. The convergence of AI-driven impersonation, ransomware extortion, and state-backed hybrid operations will increasingly blur the line between traditional cybercrime and strategic disruption. Executives, high-value companies, and critical infrastructure providers will remain primary targets, for financial extortion but also for coercive leverage in the broader political and economic context.

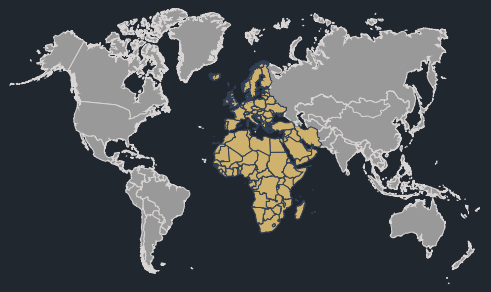
Global Insights Report

September 2025

sps
A Concentric Company

EMEA

Europe, Middle East & Africa



Ukraine

Abducted Children

Ukrainian officials allege over 19,000 children have been abducted and sent to 43 different facilities across Russia since the start of the invasion in 2022.

Mobilisation Extortion

Local citizens issued 1,600 complaints over mobilisation extortion in the first five months of 2025.

Bribary Scheme

Two soldiers were detained in Odessa in March 2025 over a $6,000 bribery scheme.

Cyberattacks

Ukrainian officials recorded 4,300 cyberattacks across Ukraine in 2024.

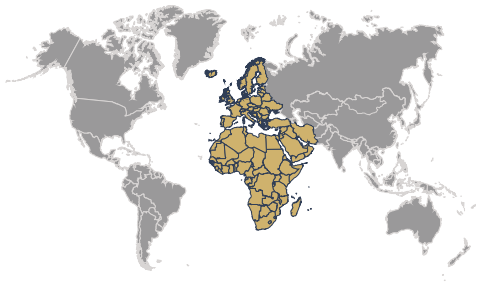
Kidnap and extortion threats are acute across Ukraine but differ sharply by geography: in the Russian-controlled east, risks stem from arbitrary detention, torture, child abductions, and systemic bribery tied to “passportisation”. In the government-held west, threats are primarily corruption-driven, involving mobilisation-related extortion targeting servicemembers and their families, protection rackets within units, and bribery schemes involving draft dodgers. Cyber extortion is a persistent parallel threat, with thousands of ransomware and data-theft incidents annually amplifying risks to both the state and private sectors.

Global Insights Report

September 2025

EMEA

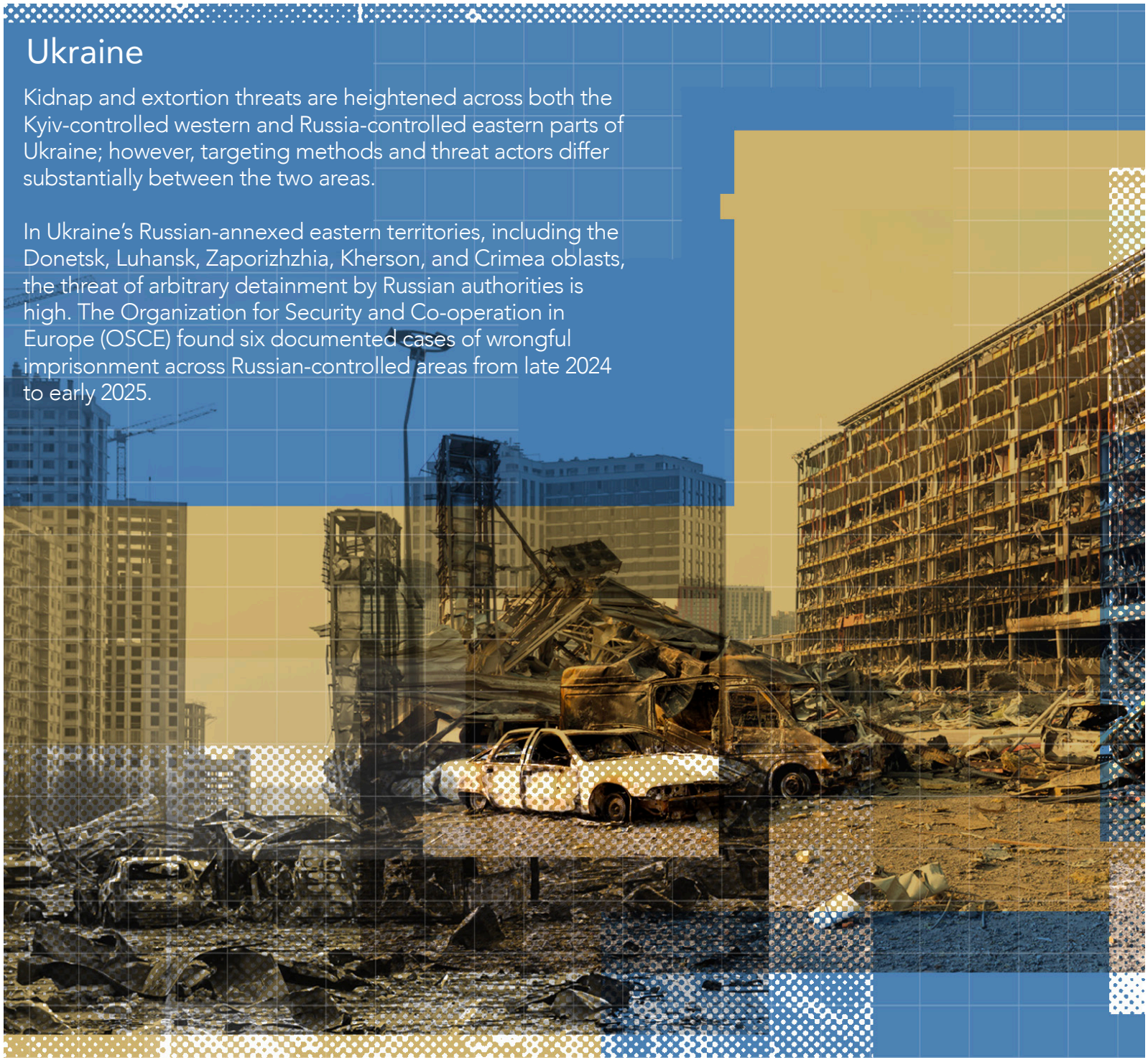
Europe, Middle East & Africa



Ukraine

Kidnap and extortion threats are heightened across both the Kyiv-controlled western and Russia-controlled eastern parts of Ukraine; however, targeting methods and threat actors differ substantially between the two areas.

In Ukraine's Russian-annexed eastern territories, including the Donetsk, Luhansk, Zaporizhzhia, Kherson, and Crimea oblasts, the threat of arbitrary detainment by Russian authorities is high. The Organization for Security and Co-operation in Europe (OSCE) found six documented cases of wrongful imprisonment across Russian-controlled areas from late 2024 to early 2025.

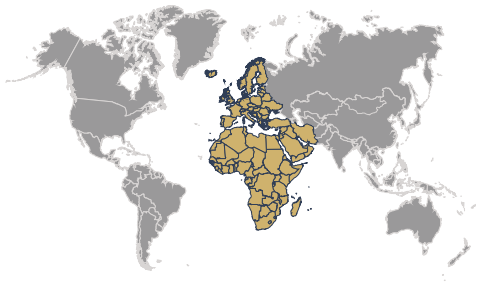


Global Insights Report

September 2025

EMEA

Europe, Middle East & Africa



Ukraine

- Victims were selected due to perceived links to the Ukrainian military, or not displaying sufficient deference to Russian occupying forces. Imprisoned individuals are not permitted contact with family or legal counsel and have been regularly taken to facilities within Russian territory and subjected to torture.

- Russian authorities are also guilty of widespread extortion, systematically targeting residents without Russian passports. Occupying forces deny Ukrainians without Russian documents passage through checkpoints unless they are able to provide a bribe – this process has furthered what President Vladimir Putin termed the "passportisation" of Russian-controlled Ukraine, by granting incentives for obtaining Russian papers.

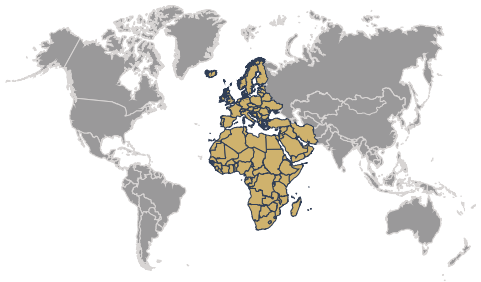
- Russian officials have also attempted cultural conversion in eastern Ukraine by conducting mass abductions of Ukrainian children. Approximately 6,000 children are confirmed to have been taken by Russian state forces into Russian territory since the invasion of February 2022, though Ukrainian authorities claim the number is closer to 19,000. The children are kept across at least 43 different facilities, some located as far east as Magdan Oblast on the Pacific coast, where "re-education" with Russian nationalist ideology and military training occurs. Ukrainian authorities claim some kidnapped children have returned to Ukraine as soldiers in the Russian army.

Global Insights Report

September 2025

EMEA

Europe, Middle East & Africa



Ukraine

In government-controlled western areas of Ukraine, kidnap and extortion threats largely involve corruption and target military personnel or cyber-infrastructure.

- Extortion related to mobilisation call-ups is particularly common, with over 1,600 complaints made to authorities over this issue in the first five months of 2025. Servicemembers and their families are both targeted by military officials abusing their power for financial gain.

- In December 2024, an investigation was launched into the 211th Pontoon Bridge Brigade's leadership team, alleged to have organized a protection racket that threatened outsiders with deployment to frontline areas.

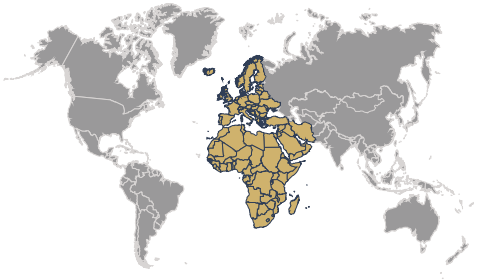
- Servicemembers have also targeted draft dodgers, extorting them in exchange for non-investigation. In March 2025, two soldiers in Odessa were detained for a $6,000 bribery scheme in which soldiers approached draft dodgers offering to remove their name from conscription wanted lists.

Global Insights Report

September 2025

EMEA

Europe, Middle East & Africa



Ukraine

Alongside military-related extortion, the cyber extortion threat has also risen substantially since the Russian invasion. Cyberattacks have increased in frequency, typically involving mass malware or ransomware attacks designed to copy sensitive information. In March 2025, three consecutive cyber attacks aimed to steal sensitive information from Ukrainian government agencies. In 2024, over 4,300 cyberattacks were reported across western Ukraine, highlighting a persistent threat to individual data security and the potential for significant cyber-extortion operations.

Global Insights Report

September 2025

Propriety Information

Contact

For more information on our
Kidnap, Ransom, Extortion and Piracy capabilities
please contact our Crisis Management Team at
cmt@sps-global.com