Securitas

Risk Intelligence Center

Annual Intelligence Estimate 2025 mid-year review

Intelligence@securitas.com

July 2025

Contents

Securitas

01

Methodology

Risk Intelligence Center

Annual Intelligence Estimate 2025 mid-year review

What was the RIC's Annual Intelligence Estimate 2025?

The Securitas Risk Intelligence Center's Annual Intelligence Estimate provides actionable intelligence for corporate security and security risk professionals for the year ahead – and beyond.

The Annual Intelligence Estimate includes a selection of corporate security issues, and key geographic considerations. The report is intended as an actionable alternative to other thematic assessments, with security decision makers in mind. It provides situational awareness for organizations in all industries and sectors, and as such is produced as a digestible high-level brief for a general audience complete with practical considerations.

If you have any questions about the report, or if you would like to discuss your specific intelligence requirements, please contact the RIC.

What is the mid-year review?

The mid-year review intends to provide organizations with a 'where are we now' for the Annual Intelligence Estimate's most significant selections, as identified by the Risk Intelligence Center.

The updated sections have been reassessed by the RIC's analysts to include an up-to-date analysis of the most prominent threats to businesses across the globe in line with the original analysis provided in the Annual Intelligence Estimate 2025, released in January.

What sections have been updated in the mid-year review?

Corporate Security

- Heightened gray-zone warfare and sabotage threaten organizations' security
- Organizations increase preparations for 'wartime scenarios'
- Executives and politicians in the crosshairs of threat actors
- Ideological insiders increasingly threaten organizations' security
- Social media exploitation fuels information disorder

Regional Security

- Changing Middle East security landscape as Iranian regional doctrine fractured
- US election result influences political partisanship
- Russia escalates sabotage campaign across Europe

Recent developments and upcoming flashpoints

- AMEA
- Americas
- Europe

Approach

The RIC employs an all-source intelligence strategy, utilizing all available and appropriate sources of intelligence based on the intelligence requirement(s).

This approach combines the expertise of our in-house analysts, the global network of the Securitas organization, third parties and partners, and cutting-edge technology for open-source intelligence (OSINT), to produce the highest quality finished intelligence. Inclusion in the Annual Intelligence Estimate is not a statement that any of these scenarios will occur, but that the potential exists for the threat to manifest and that the threat should be considered when performing security and safety reviews and risk assessments.

Threat levels

This report uses the RIC's threat level system to score threats on a 1-5 scale based on the assessed likelihood and severity, and / or intent and capability.

THREAT LEVELS	
5 – EXTREME	Very high / extreme threat. Review and respond if required.
4 – HIGH	High / major threat. Consider taking appropriate action.
3 – MODERATE	Moderate threat. Maintain awareness, consider precautions.
2 – LOW	Low / limited threat. Be advised.
1 – VERY LOW	Very low / insignificant threat. For awareness.

Language of probability

This report uses the RIC's language of probability to provide an assessment of the likelihood of a threat manifesting, based on probability, using a percentage, fraction, or ratio as a baseline. This helps to provide context and clarity, and helps promote a standardized understanding of assessment and terms used.

LANGUAGE OF PROBABILITY							
Term:	Remote	Highly unlikely	Unlikely	Realistic possibility	Likely / Probable	Highly likely	Almost certain
Probability:	0-5%	10-20%	25-35%	40-50%	55-75%	80-90%	95-99%

Intelligence Cut Off Date (ICOD):	2359hrs UTC 30 June 2025

02

Corporate Security

Annual Intelligence Estimate 2025 mid-year review – Corporate Security

Heightened gray-zone warfare and sabotage threaten organizations' security

The use of hostile strategies / tactics by state and non-state actors when opposing actors are not engaged in traditional conflict or open war – but peace is also not being observed – known as gray-zone warfare (GZW), is an evolving threat that is increasingly being utilized by a diverse range of threat actors as geopolitical tensions increase. GZW targets often includes military sites, transportation nodes (airports, roads, ports), logistics facilities, government services, and utility infrastructure (energy, water, undersea cables). GZW and sabotage are increasingly likely to result in significant disruption, including mass casualty incidents, supply chain disruption, IT / communications outages, impacting critical national infrastructure (CNI), industries, businesses, and individuals.

Update	Condition
The threat posed by sabotage and other GZW operations has continued to increase during the first half of 2025 as rising global tensions continue to be driven by further escalations of ongoing conflicts in the Middle East and Ukraine, increasing geopolitical competition, hostilities between China and Taiwan, and international disputes surrounding trade and economic policy. Reports of unidentified drones being sighted over pieces of CNI gained attention in 2024, particularly over military installations. This trend has continued in 2025 with unidentified drone sightings being reported above military sites and CNI across various European countries, including Denmark, Germany, Norway, and the UK, throughout January alone. The sightings occurred amid persistent concerns surrounding the security of critical subsea infrastructure due to such infrastructure being damaged under suspicious circumstances throughout 2024 and 2025.	Worsening

Recent developments (SIGACTs)

Date	Location	Description
8 Jan	Baltic Sea	NATO announced plans to launch a maritime "Enhanced Vigilance Activity" operation in the Baltic Sea to protect underwater CNI due to GZW concerns.
14 May	Netherlands	The Dutch military raised its alert level from 'Alpha' to 'Alpha Plus,' citing an "increased threat" of sabotage within or near its territory.
6 Jun	Sweden	Swedish authorities announced they were investigating damage to ~30 telecommunications masts along the E22 highway as potential sabotage.

- ✓ Assess exposure to scenario-based threats in the context of organizations, including direct (i.e. targeting by most likely threat actors and their motivation, intent, and capability) and indirect targeting (i.e. impacts arising from loss of key services / infrastructure).
- ✓ Proactively monitor for potential escalations. Utilize intelligence capabilities to assess and monitor threats during heightened periods of threat / unrest.
- ✓ Utilize accurate sources of information and seek to identify and avoid misinformation and disinformation. Consider sharing reliable sources with employees to avoid unnecessary panic from misreporting.

Indicators

- Increasingly frequent high-profile instances of suspicious accidents (fires / infrastructure damage, etc) impacting CNI and sensitive sites.
- Governments increasing terror threat levels, issuing warnings about hostile GZW / sabotage / hybrid action campaigns.
- Governments allocate additional resources to domestic security services and provide training to the private sector.
- Heightened observance of cyber threat activities from state and state-backed cyber threat actors, primarily China, Russia, and North Korea targeting government and private organizations.

Implications

- Private organizations operations are increasingly disrupted and security compromised, particularly those operating CNI or in sensitive industries such as defense.
- States are encouraged to allocate additional resources to their security forces and implement training to raise awareness / increase resilience to GZW operations.
- Threat actors increasingly exploit divisive social issues as part of GZW operations to cause unrest and undermine political systems and government institutions.
- Organizations forced to heighten security measures (cyber and physical) to combat rising threats.

Organizations increase preparations for 'wartime scenarios'

Organizations are increasingly preparing for 'wartime scenarios' due to geopolitical competition, frequent sabotage, and other gray-zone warfare (GZW) incidents, and threats of global conflict surrounding flashpoints such as Gaza, Taiwan, and Ukraine. Numerous countries have increased defense spending, committed to collaborative readiness projects, and shifted to a 'wartime mindset', including NATO. Businesses and organizations are increasingly facing the heightened threat of being targeted directly as well as by secondary / tertiary impacts of state-backed action.

Update	Condition
Preparations for 'wartime scenarios' have continued to advance in 2025 as the geopolitical landscape has become increasingly volatile as a result of the continued conflicts in Gaza and Ukraine being exacerbated by the outbreak of conflict between Israel and Iran in June. NATO presented plans to increase its defense spending target from 2% to 5% of GDP during its annual summit in June, while the Baltic States, Finland, Poland, and Ukraine announced intent to / have withdrawn from the Ottawa Convention, which bans the stockpiling, procurement, and use of anti-personnel landmines, in response to the increased threat posed by Russia. Notably, private organizations are increasingly being seen as legitimate targets by nation states, with a Boeing office in Kyiv, Ukraine, being deliberately targeted in a Russian drone strike overnight on 9-10 June and a Microsoft building in Be'er Sheva, Israel, reportedly being intentionally targeted in an Iranian missile strike on 20 June.	Worsening

Recent developments (SIGACTs)

Date	Location	Description
10 Jan	Norway	The government presented a total preparedness plan to prepare citizens for the *"worst-case scenario"* and other security challenges facing the country.
20 Jan	UK	The Home Office issued new guidelines for private security personnel to detect threats posed by clients employed by hostile foreign states in line with the National Security Act 2023.
13 Jun	Baltic States	Estonia, Latvia, and Lithuania signed a joint strategy for mass evacuations in the event of a crisis, including measures to streamline information exchange and ensure vulnerable groups are not left behind.
24 Jun	UK	The country's latest National Security Strategy stated it must *"actively prepare"* for a potential wartime scenario on the domestic front, citing increased threats from Iran and Russia.

- ✓ Organizations, especially those operating within commonly targeted sectors, are advised to raise employee awareness of potential threats and simultaneously improve their security posture.
- ✓ Organizations are advised to ensure they are not engaging in business or communicating with businesses or assets as they could be exposed to OPSEC risks and domestic scrutiny.
- ✓ Organizations should consider developing and regularly reviewing risk management plans to be deployed in the event of conflict escalation.

Indicators

- State actors such China and Russia are increasingly implicated in GZW operations targeting businesses and organizations.
- World powers continue to increase defense spending, announce new joint defense projects, and warn of 'wartime measures.'
- Governments issue new civil guidance regarding preventative measures that can be taken ahead of military conflict.
- Private sector organizations develop security and resilience capabilities in line with government guidance.
- Governments continue to encourage businesses to diversify supply chains from adversarial states.

Implications

- Relations with businesses in adversarial states such as China and Russia (and their partners) deteriorate, forcing operational challenges.
- Supply chains and sources of critical materials / essential commodities are diversified, presenting new commercial opportunities, but also likely increased costs.
- Businesses and public institutions are required to improve their security postures, especially in relation to cyber threats, inciting increased financial costs.
- Uncertainty surrounding armed conflict undermines global investor confidence, reducing foreign investment.

Annual Intelligence Estimate 2025 mid-year review – Corporate Security

Executives and politicians in the crosshairs of threat actors

Increasing threats to organization executives have consistently correlated with workplace grievances and ideological / activist causes, with recent violent incidents highlighting the current heightened threat actor motivation and capabilities to cause physical harm to executives, which is expected to persist into 2025. The threat of high-profile individuals, such as senior executives and politicians, being targeted by malicious threat actors has persisted amid ongoing geopolitical tensions with China, Iran, and Russia and their exploitation of global internal divisions via foreign state actors.

Update	Condition
The assassination of United Healthcare (UHC) CEO Brian Thompson in December 2024 and the surrounding rhetoric sparked heightened concerns about executive safety globally. While the legal case surrounding Thompson's suspected killer, Luigi Mangione, continues to serve as a driver of social unrest and left-wing / anti-capitalist sentiments, no 'copycat' killings have taken place in the first half of 2025. Despite this, executive protection has continued to be an emerging issue, underscored by threat events such as contact information and personal details of hundreds of executives employed by organizations across multiple industries, primarily in the US, being listed on a website titled 'CEO database' associated with the domain name 'luigiwasright.com', and a series of cryptocurrency CEO's being kidnapped in France. Additionally, instances of activists using open-source platforms to gather information about the presence of certain individuals / companies at events for the purpose of confronting executives have become more frequent. This is likely being driven by activists seeking to maximize publicity for their cause by disrupting events and believing executives / politicians are more likely to implement policy changes when directly confronted.	**Stable**

Recent developments (SIGACTs)

Date	Location	Description
10 Jun	Colombia	Criminals fatally shot and robbed Karin Sefair Calderon, the coordinator prosecutor of Fusagasuga and Sumapaz in Cundinamarca Department, after he withdrew money from an ATM in a busy shopping center.
7 Apr	Global	Contact information and personal details of hundreds of executives employed by organizations across multiple industries, primarily in the US, were listed on a website titled 'CEO database' associated with the domain name 'luigiwasright.com', a reference to Luigi Mangione, the suspected killer of the CEO of US medical care provider UHC.

- ✓ Develop security frameworks for VIPs to ensure protection amid increasing risks to life and malicious influence. Carry out the operations security (OPSEC) cycle with a variety of internal stakeholders about the cyber presence of the organization online, including on social media.
- ✓ Malicious or threatening communications should be notified to authorities, with persistent / substantial targeting potentially leading to the implementation of court injunctions or restraints to limit future targeting.
- ✓ Be aware of the potential risks of making public or official statements regarding provocative or controversial actions, as these may be exploited by threat actor groups to engage in hostile or threatening actions.

Indicators

- Increased attempts to assassinate or inflict harm to executives / politicians or other VIPs.
- Changes in security protocols and increased measures for executives / politicians and their associates or assets.
- Persistent advertisement of online campaigns targeting businesses / governments departments related to VIPs, including malicious communications using provided templates.
- Increased reports of politicians being exploited for espionage / agents of influence via honeytraps by foreign state actors.

Implications

- Business operations delayed / canceled due to security precautions amid threats and risk of attacks against VIPs.
- Online services for businesses and government institutions disrupted by cyber attacks or spread of mis / dis / malinformation via social media.
- Businesses' brand reputations damaged and impact on business relations due to threats of targeting within supply chains.
- Businesses / government departments increasing security budgets to match appropriate VIP protection with heightened threat landscape.

Annual Intelligence Estimate 2025 mid-year review – Corporate Security

Ideological insiders increasingly threaten organizations' security

Ideologically motivated insider threats have become increasingly common as widely popular activist causes, personal grievances, and political differences have motivated employees to target organizations and supply chains. Major flashpoints in activism, ranging from geopolitical tensions to environmental causes, have greatly contributed to the growth of activist movements, which have been increasingly recruiting employees to target their organizations, with this trend likely to continue into 2025.

Update	Condition
The threat posed by ideological insiders has continued to increase over the last six months, caused by increasing inter-state competition and a growing / intensifying activism landscape that is primarily being driven by ongoing conflicts in the Middle East and increasing social / political polarization over a range of issues such as environmentalism and immigration.Additionally, activist groups such as No Tech for Apartheid and No Azure for Apartheid have increased calls for organizational insiders with ideological sympathies to take action, and have continued producing content specifically targeted at insiders of certain organizations. The risk posed by ideological insiders will almost certainly continue to be exacerbated by technology's increasing ability to enable motivated actors to take action that can threaten an organization's security with fewer risks of identification or consequences, and the increasing utilization of the cyber domain among threat actors.	Worsening

Recent developments (SIGACTs)

Date	Location	Description
31 Jan	US	Former US Federal Reserve Adviser John Harold Rogers was arrested for allegedly conspiring to steal and share confidential information with individuals linked to China's intelligence services.
19 May	US	Pro-Palestine activists with No Azure for Apartheid (NoAA) disrupted a keynote address by Microsoft CEO Satya Nadella at the Microsoft Build 2025 conference. Notably, one of the activists was a firmware engineer with Microsoft Azure Hardware Systems and Infrastructure.
10 Jun	Taiwan	Taiwanese prosecutors indicted four former government officials on charges of espionage for China, seeking prison sentences of over 18 years. All four defendants were previously affiliated with the ruling Democratic Progressive Party (DPP). The charges include allegedly passing classified national security information to Chinese authorities.

- ✓ Organizations are advised to develop effective insider threat identification and detection programs, focusing on behavioral indicators / exploitable traits, repeated security violations, and unnecessary attempts to become involved in sensitive or restricted areas, combining human resources and technology.
- ✓ Organizations should maintain situational awareness to pre-emptively identify issues or trends that may see an increase in insider threats, whether targeting the organization specifically, its partners, or the supply chain.
- ✓ Ensure employees are aware of reporting procedures for suspicious behavior and activity within the workplace.

Indicators

- Employee groups, unions, or individuals voice politically motivated disagreement with their organization's operational practices / policies.
- Ongoing popular flashpoints for activism continue to target private organizations and subsequently act as motivation for ideological insider threats.
- Threat actors maintain social media campaigns, outreach, and calls to action directed at individuals employed by target organizations.
- Employees engaging or promoting activist / ideological content on social media, including material critical of their employer.

Implications

- Leakage of sensitive data by insider threats posing security threats, including within supply chains, and possible reputational damage.
- Potential for individuals / groups of like-minded ideologically driven employees to disrupt daily operations or sabotage their workplace.
- Reputational threat stemming from employees publicly criticizing their organization.
- Potential cost of increased security and monitoring measures within the organization to identify and prevent insider threat disruptions.
- Possible use of violent tactics is likely to result in casualties, posing security threats to the workforce.

Social media exploitation fuels information disorder

There are three main types of information disorder: misinformation, disinformation, and malinformation. As we move into 2025, information disorder is expected to remain a significant threat to organizations, with threat actors continuing to circulate false, misleading, or harmful information primarily related to organizations operations, business partnerships, and their executives. This will particularly be the case in the context of societal, governmental, and geopolitical flashpoints, impacting businesses in various ways including reputational, financial, and operational damage.

Update	Condition
Recent global conflicts and significant flashpoints have highlighted the increasing importance being placed on the exploitation and control of social media by both state and non-state actors and the role mis / dis / malinformation has in shaping the information landscape during emerging incidents and geopolitical uncertainty. During the four-day India-Pakistan conflict in May, Meta reportedly restricted access to one of the most followed Muslim news sources on Instagram, @Muslim, for users in India at the request of the Indian government, while social media platform X received executive orders from the Indian government requiring it to block more than 8,000 accounts in India. Additionally, India blocked access to numerous Pakistani social media accounts, including YouTube channels of Pakistani news outlets and the Instagram accounts of prominent Pakistani figures such as former Prime Minister Imran Khan. This was further demonstrated during the Iran-Israel conflict, as pro-Iranian sources claimed footage of a Chilean pilot ejecting from her plane was an Israeli pilot being intercepted over Iran / disseminated videos generated by artificial intelligence (AI) claiming to show the impact of Iranian strikes on Israel. Likewise, pro-Israel accounts shared old footage of protests in Iran, aiming to spread uncertainty about the country's political stability.	Worsening

Recent developments (SIGACTs)

Date	Location	Description
26 May	UK	~47 people were injured, including 27 hospitalized, after a vehicle drove into a crowd of football fans during a celebration parade in Liverpool. Notably, police were quick to provide details about the suspect in an apparent attempt to quell claims he was inspired by Islam or was an immigrant.
17 Jun	US	Research showed social media and video networks have become the main source of news in the US for the first time, overtaking traditional TV channels and news websites, increasing concerns over the spread of mis / dis and malinformation.

- ✓ Ensure that incident response plans are in place and regularly rehearsed to effectively address instances of information disorder, ensuring that official communications are disseminated efficiently to counter false narratives.
- ✓ Consider the reliability and credibility of unofficial sources and social media channels, and utilize recognized fact-checking platforms to identify potential instances of information disorder.
- ✓ Consider employing authentication techniques in public-facing communications, such as digital watermarking, which can be used to verify authenticity.

Indicators

- Significant elections or votes are likely to trigger a surge in information disorder.
- Public health crises spark misinformation campaigns, especially around vaccinations, fueling anti-vaccine movements and undermining public health guidance.
- Media coverage of localized violent crimes often spreads information disorder, vilifying specific ethnic or religious minority groups.
- Rising geopolitical tensions drive state-backed campaigns that spread information disorder.

Implications

- Organizations may face significant reputational harm as misinformation or disinformation campaigns target the brand or executives.
- Rising use of violent tactics targeting high-profile individuals, including organizations' executives, fueled by information disorder is highly likely to pose safety and security threats, including during business travel.
- Rising concerns over information disorder may lead to stricter regulations and compliance requirements, particularly in areas such as data privacy and content transparency.
- Organizations may be required to invest in crisis management resources to monitor, identify, and respond to instances of misinformation campaigns.

03

Regional Security

Changing Middle East security landscape as Iranian regional doctrine fractured

Threat actors continued to exploit Middle East tensions in 2024, but the Iranian-led Axis of Resistance (AOR) has been disrupted by Israeli and allied efforts and most recently fractured by the fall of the AOR's division in Syria: Bashar al-Assad's regime. Iran is reeling from significant blows to the AOR, particularly as Bashar's Syria was a primary host for Iran to supply proxy militant groups in Lebanon, Iraq, and elsewhere. Iran will likely pursue other forms of deterrence against Israel and the US, including increased aggressive posture and signaling around Iran's nuclear capabilities and reevaluating its AOR-reliant defense, shifting the regional security landscape.

Update	Condition
The security landscape in the Middle East has significantly deteriorated over the last six months. While five rounds of nuclear talks between Iran and the US from April to May were a source of optimism for many, Israel launched pre-emptive strikes on Iranian nuclear facilities, military installations, and senior leadership on 13 June, claiming Iran already had the capacity to produce nine nuclear bombs. These strikes triggered a 12-day conflict, which involved the US directly attacking three Iranian nuclear facilities on 22 June and Iran responding by threatening to close the Strait of Hormuz and launching missiles at a US base in Qatar before a ceasefire was announced on 24 June. Notably, the conflict showed increased strains among the AOR. While Israel was unable to kill Iranian Supreme Leader Ayatollah Ali Khamenei or incite regime change, several key nuclear scientists and senior commanders, including the Chief Commander of the Islamic Revolution Guards Corps (IRGC), Major General Hossein Salami, second-in-command of the armed forces, Mohammad Bagheri, and the head of IRGC intelligence, Mohammed Kazemi were killed, almost certainly damaging the Iranian regime.	Worsening

Recent developments (SIGACTs)

Date	Location	Description
5 Mar	Gaza Strip	A ceasefire between Israel and Hamas collapsed when Israel resumed military operations in the Gaza Strip after claiming Hamas was preparing to launch attacks and had refused to release hostages during negotiations.
13 Jun	Iran	Israel launched pre-emptive strikes on Iranian nuclear facilities, military installations, and senior leadership, claiming Iran already had the capacity to produce nine nuclear bombs.
22 Jun	Iran	The US attacked three Iranian nuclear facilities, leading to Iran threatening to close the Strait of Hormuz and launching missile strikes on a US base in Qatar.

- ✓ Develop detailed business continuity plans that account for various disruption scenarios, including maritime route closures, regional banking disruptions, and supply chain interruption, for businesses in the region and internationally.
- ✓ Review and enhance cyber security measures to protect against state-sponsored attacks, particularly focusing on critical infrastructure and sensitive data.
- ✓ Maintain awareness of the potential for Middle East tensions to continue to motivate threat actors internationally, including activists and terrorists / extremists.

Indicators

- Changes in frequency and sophistication of AOR attacks on US interests across the Middle East, particularly in Iraq and Syria.
- Rising incidents of maritime security threats in the Red Sea and Persian Gulf, particularly targeting vessels linked to Israel or Western interests.
- Growth in anti-Western rhetoric and recruitment activities by Iranian-backed groups, especially in areas with reduced US presence.
- Shifts in US troop movements and resourcing to implement renewed pressure on Iran.

Implications

- Rapid shifts in regional dynamics following the January 2025 US transition of power, providing an unpredictable business landscape.
- Shift in Iranian regional doctrine as the AOR is disrupted and fractured to new deterrents.
- Continued disruption to regional supply chains and shipping routes, particularly affecting energy, and maritime sectors.
- Strategic shift required in business operations as US military withdrawal creates new security dynamics, particularly in Iraq and Syria.
- Western organizations face increased hostility and possible targeting in areas with strong support for Palestine / Iran.

US election result influences political partisanship

The US political landscape is becoming increasingly polarized as explicit socio-economic factors, underlying divisions, and geopolitical inputs, stimulate partisan political views that politicians, businesses, media, and malicious threat actors are further exploiting. Resultingly, discord between members and supporters of opposing political parties is manifesting through increasingly hostile views, commentary, and actions. This discontent has also recently been linked to violent and terror-related incidents across the US, with this threat expected to become increasingly prevalent throughout 2025 as the Trump administration comes into office.

Update	Condition
Emotive and socially divisive issues such as immigration, the Gaza-Israel conflict, President Joe Biden's health, and the attempted assassination of Donald Trump, resulted in the 2024 presidential election cycle continuing the trend of political polarization and partisanship in the US. Since Trump's presidential inauguration in January, his policies and approaches to geopolitical challenges have driven domestic criticism and unrest. Notable drivers include but are not limited to: the use of the 1798 Alien Enemies Act to facilitate the deportation of organized crime group (OCG) members, ongoing attempts to cancel birthright citizenship, Immigration and Customs Enforcement (ICE) agency activity and deportations, clashes with universities over several issues, the implementation of global tariffs, military conflicts involving Israel, US strikes on Iranian nuclear facilities, cuts to federal funding, anti DEI initiatives, and territorial claims being made on Canada and Greenland. Additionally, instances of politically inspired extremism have occurred in recent months. This includes six people being injured when a man threw incendiary devices at a crowd holding a pro-Israel vigil in Boulder, Colorado, on 1 June, and two Israeli Embassy staffers being shot and killed at a Jewish event in Washington DC on 21 May.	**Stable**

Recent developments (SIGACTs)

Date	Location	Description
5 Feb	US	Nationwide protests were organized outside state capitol buildings and other locations as part of the 50501 Movement in response to executive orders issued by President Donald Trump and the Project 2025 political initiative. 50501 has held several nationwide and localized mobilizations during Trump's first months in office.
14 Jun	US	~1,500 'No Kings' protests were held across the US to denounce President Donald Trump's alleged authoritarian policies and reject the organization of a military parade as a sign of "national defiance", amid national unrest sparked by ICE raids and subsequent rioting in Los Angeles.

- ✓ Organizations are advised to maintain awareness of the political calendar and the potential for unrest to occur as a result.
- ✓ Businesses should consider reviewing their portfolios to identify any elements that could be perceived as being connected to a political party / group and could be targeted during increased unrest.
- ✓ Organizations are advised to maintain an understanding of information disorder and the information landscape, especially regarding information on contentious issues, and ensure employees are educated on potential impacts.

Indicators

- The stance of political parties on key issues is generally in opposition resulting in less bipartisan legislation passing.
- Activist actions related to divisive issues force operational changes for businesses in all sectors.
- Isolated incidents of political violence occur alongside political flashpoints.
- Information disorder contributing to political violence and partisan views is identifiable.
- Those on the extremes of the political spectrum are active and widespread in the political space, especially online.

Implications

- Organizations will likely experience security threats related to political violence and unrest
- Employee morale within certain organizations will likely become further politicized and, in some cases, hostile.
- Organizations with connections to political parties / figureheads will likely be targeted.
- Links between certain domestic and foreign businesses will likely degrade due to political destabilization and insecurity.
- Possible violent or terror / extremist incidents fueled by the domestic political landscape result in mass casualty events impacting security in effected states and country-wide.

Russia escalates sabotage campaign across Europe

Russia continues to conduct espionage and sabotage actions across Europe as part of a coordinated gray-zone warfare (GZW) campaign targeting critical infrastructure and organizations engaged in commercial relations with Ukraine. Further sabotage actions are highly likely to persist as inter-state tensions continue to rise regarding Western support for Ukraine. GZW is used to thwart, destabilize, weaken, or gradually attack adversaries, allowing the perpetrator to remain anonymous or deny responsibility using conventional and unconventional means and proxies.

Update	Condition
While diplomatic efforts to bring a peaceful resolution to the Russia-Ukraine conflict have significantly increased since US President Donald Trump returned to office in January, the short-term likelihood of peace remains highly unlikely. Russia has continued its GZW campaign across Europe, primarily targeting countries that are providing support to Ukraine through financial means, directly providing military equipment, or sanctioning Russia, as well as private organizations in these countries. Additionally, private organizations with direct links to supporting Ukraine's military capabilities and organizations operating in sectors deemed critical to national security, such as aerospace and defense, technology, telecommunications, and other pieces of CNI, remain priority targets.	Worsening

Recent developments (SIGACTs)

Date	Location	Description
24 Mar	Austria	The Directorate for State Security and Intelligence announced it uncovered a widespread Russian disinformation campaign seeking to increase pro-Russian and anti-Ukrainian sentiments in the country, following the beginning of an investigation into a Bulgarian national accused of espionage.
23 May	UK	Counterterrorism police reportedly began investigating potential Russian involvement in a series of arson attacks on properties connected to Prime Minister Sir Keir Starmer.
11 Jun	Sweden	Authorities announced the media outlet SVT, critical infrastructure, banks, and other organizations were reportedly targeted in a series of Distributed Denial of Service (DDoS) attacks over the past three days, prompting Prime Minister Ulf Kristersson to claim the country is *"under attack."*
26 Jun	Germany	Footage of at least six German military trucks being burned at a MAN repair facility in Erfurt was disseminated by a pro-Russian Telegram groups, prompting investigations into possible sabotage.

- ✓ Organizations commonly previously targeted sectors are advised to maintain an enhanced security posture and take adequate provisions to mitigate the risk of damages to assets and personnel.
- ✓ Maintain contact with authorities and follow advice on preventative measures to safeguard assets and facilities.
- ✓ Increase patrolling and monitoring of vulnerable business areas which will possibly be exploited by threat actors.
- ✓ Assess potential supply chain impacts caused by damage / disruption of CNI or specific sector essential for business operations.

Indicators

- Increasing reports of suspected Russian sabotage as observed across Europe – from public and private sectors – including those associated with other nation-state-back threat actors (China, Iran, North Korea).
- Increased targeting of Russian military assets using Western-supplied weapons.
- Russian authorities maintaining plausible deniability of actions.
- Rising exploitation on insider threats, including within supply chains, to heightened impacts of sabotage attempts.

Implications

- Heightened cyber and physical threats, increasing the risk of asset damages and prolonged operational disruptions within the public and private sectors.
- Increasing hostile tactics are likely to pose a heightened risk of civilian casualties.
- Heightened security requirements, and subsequent costs, for at-risk businesses / industries.
- Further restrictions on business relations with Russian organizations, impacting supply chains.
- Possible conflict spread from Ukraine to other European states, significantly impacting regional stability and business operations.

06

Global Security – 2025 Recent developments and upcoming flashpoints

Annual Intelligence Estimate 2025 – Global Security – Recent developments and upcoming flashpoints

Securitas

2025 Recent developments and flashpoints - AMEA

JANUARY

M23 rebels captured several cities in the eastern Democratic Republic of the Congo throughout January, inflaming regional tensions and disrupting mining operations critical to global supply chains.

FEBRUARY

Australia sanctioned the right-wing online terror network 'Terrorgram' to combat rising antisemitic attacks and online extremism on 3 February. Sanctions were also renewed on other right-wing groups, namely, the National Social Order, the Russian Imperial Movement, the Sonnenkrieg Division, and The Base.

MARCH

A ceasefire between Israel and Hamas collapsed on 5 March when Israel resumed military operations in the Gaza Strip after claiming Hamas was preparing to launch attacks and had refused to release hostages during negotiations.

APRIL

South Korea's Constitutional Court unanimously upheld the impeachment of President Yoon Suk Yeol on 4 April, after ~three months of uncertainty and political instability caused by his declaration of martial law in December 2024. Yoon's impeachment triggered snap presidential elections.

MAY

Tensions between India and Pakistan culminated in a four-day low-intensity conflict. India struck nine targets allegedly affiliated with terror groups in Pakistan and Pakistan-administered Kashmir as part of 'Operation Sindoor' on 7 May, while Pakistan struck Indian Air Force installations and conducted cyber attacks on 10 May before a ceasefire was announced.

JUNE

Israel launched airstrikes targeting Iranian nuclear facilities, military installations, and senior leadership on 13 June. The strikes prompted retaliatory missile and drone strikes against targets in Israel, leading to a 12-day conflict which saw the US strike three Iranian nuclear facilities on 22 June and Iran threaten to close the strategically important Strait of Hormuz.

JULY

- **1 Jul:** Anniversary of the founding of the CCP
- **4 Jul:** Ashura Eve
- **12 Jul:** Anniversary of the Israel-Lebanon 2006 War
- **14 Jul:** Iraqi Republic Day

AUGUST

- **1 Aug:** George Habash Birthday
- **3 Aug:** Tisha'Bav
- **14 Aug:** Arbaeen
- **25 Aug:** Anniversary of the 2018 Rohingya Genocide
- **30 Aug:** Anniversary of the US withdrawal from Afghanistan

SEPTEMBER

- **11 Sep:** Anniversary of the 2012 Benghazi attack
- **16 Sep:** Martyr's Day
- **21 Sep:** Anniverary of the 2013 Westgate Mall terror attack

OCTOBER

- **1 Oct:** Anniversary of the death of Armita Geravand
- **7 Oct:** Second anniversary of the 7 October attack
- **16 Oct:** Israeli National Remembrance Day
- **29 Oct:** Turkish Republic Day

NOVEMBER

- **1 Nov:** Anniversary of the 1954 Algerian Revolution
- **2 Nov:** Balfour Day
- **15 Nov:** Palestinian Independence Day
- **26 Nov:** Anniversary of the 2008 Mumbai Attacks
- **27 Nov:** Anniversary of the founding of the PKK

DECEMBER

- **15 Dec:** Anniversary of the completion of the Iraq War
- **18 Dec:** Anniversary of the US military withdrawal from Iraq
- **19 Dec:** Goa Liberation Day
- **21 Dec:** AFCON football tournament
- **31 Dec:** Anniversary of the 2019 attack on the US embassy in Baghdad

Annual Intelligence Estimate 2025 – Global Security – Recent developments and upcoming flashpoints

2025 Recent developments and flashpoints - Americas

JANUARY

US President Donald Trump was inaugurated on 20 January, marking his official return to office after winning the 2024 presidential election. Trump issued 26 executive orders, 12 memoranda, and four proclamations during his first day in office, covering a wide range of policy areas.

FEBRUARY

Latin American lawmakers raised security concerns after the US designated eight cartels as foreign terrorist organizations on 20 February. The measure was taken as part of US President Donald Trump's plan to stop the flow of immigrants and drugs across the Mexico-US border.

MARCH

Brazil's Supreme Court determined that former President Jair Bolsonaro will face criminal prosecution on 26 March for plotting a coup and instigating unrest to stay in power during the inauguration of President Luiz Inacio Lula da Silva in 2023.

APRIL

US President Donald Trump announced "reciprocal tariffs" on 180 countries on 2 April, intended to revive the US economy. Countries faced a minimum rate of 10%; however, many countries, including key trading partners such as China, the EU, India, and Japan, received significantly higher individualized rates. These rates were based on the US's trade deficit and other trade-related factors.

MAY

13 people were killed on 4 May after being kidnapped by informal miners linked to an organized crime group (OCG) in Peru's Pataz province on 26 April. Violence associated with informal mining led to the suspension of mining activities on 5 May, which had significant economic implications and resulted in a province-wide strike on 5 June.

JUNE

Violent unrest broke out in multiple cities across the US following Immigration and Customs Enforcement (ICE) raids in Los Angeles on 6 June. US President Donald Trump deployed the National Guard and Marines to Los Angeles to quell the unrest against the wishes of city and state leadership.

JULY

- 1 Jul: Canada Day
- 4 Jul: US Independence Day
- 13 Jul: Anniversary of the founding of the BLM Movement
- 18 Jul: Anniversary of the 1994 AMIA bombing

AUGUST

- 3 Aug: Pride Vancouver
- 12 Aug: Anniversary of the 2017 Charlottesville vehicle attack
- 17 Aug: Bolivian general election
- 26 Aug: US Open tennis tournament

SEPTEMBER

- 1 Sep: Labor Day
- 7 Sep: Brazilian Indepndence Day
- 11 Sep: Anniversary of the 9/11 terror attacks
- 21 Sep: Climate Week NYC

OCTOBER

- 1 Oct: Anniversary of the Las Vegas Shooting
- 9 Oct: Ecuadorean Independence Day
- 13 Oct: Canadian Thanksgiving
- 17 Oct: Argentine Loyalty Day
- 19 Oct: Anniversary of the 2019 Chilean Constitution protests

NOVEMBER

- 2 Nov: Day of the Dead
- 10 Nov: COP30 summit
- 15 Nov: Brazilian Republic Day
- 20 Nov: Argentine National Soveringty Day
- 20 Nov: Mexican Revolution Day
- 27 Nov: US Thanksgiving

DECEMBER

- 1 Dec: Cyber Monday
- 4 Dec: Anniversary of the assassination of UnitedHealthcare CEO
- 7 Dec: Pearl Harbour Remembrance Day
- 10 Dec: Argentine Democracy Restoration Day
- 12 Dec: Our Lady of Guadeloupe Day

Annual Intelligence Estimate 2025 – Global Security – Recent developments and upcoming flashpoints

Securitas

2025 Recent developments and flashpoints - Europe

JANUARY

NATO announced plans to launch an 'Enhanced Vigilance Activity' operation in the Baltic Sea to protect underwater critical national infrastructure (CNI) on 8 January. The operation, named Baltic Sentry, was announced amid increasing concerns about threat actors associated with hostile states, including China and Russia, operating in the region.

FEBRUARY

The Russia-Ukraine conflict marked its third anniversary, with leaders from various Western nations visiting Kyiv to mark the anniversary and reaffirm their support for Ukraine. The anniversary was preceded by renewed efforts to negotiate a peaceful resolution to the conflict by US President Donald Trump, which involved Russia and the US holding bilateral talks in Saudi Arab.

MARCH

The largest anti-government rally in modern Serbian history took place in Belgrade on 15 March, following four months of disruptive student-led protests. ~325,000 protestors from across the country are believed to have taken part despite railways being suspended due to an alleged bomb threat. Prime Minister Milos Vucevic resigned days after the protest.

APRIL

Portugal and Spain experienced the largest power outage in Europe in the last ~20 years on 28 April. The outage halted metro systems, disabled traffic signals, suspended rail services, and disrupted airports / telecommunications. Spain reported at least three deaths and estimated economic losses at $1.8 billion.

MAY

The far-right Alternative for Germany (AfD) political party was classified as a *"proven right-wing extremist organization"* on 2 May. The designation did not ban the AfD as a political organization but allows authorities to increase surveillance.

JUNE

The second round of the Polish Presidential election was held on 1 June, with nationalist candidate Karol Nawrocki beating Rafal Trzaskowski, representing Prime Minister Donald Tusk's Civic Platform party, by ~1.5% of votes.

JULY

- **3 Jul:** Belarusian Independence Day
- **5-27 Jul:** Tour de France
- **14 Jul:** Bastille Day
- **15 Jul:** Ukrainian Statehood Day
- **18 Jul:** Roay Air Tattoo

AUGUST

- **11 Aug:** XR Norway campaign period
- **14 Aug:** Anniversary of Bosnian femicide protests
- **18 Aug:** XR Norway mass mobilization
- **24 Aug:** Notting Hill Carnival

SEPTEMBER

- **4 Sep:** International Animal Rights Conference
- **8 Sep:** Norwegian parliamentary elections

OCTOBER

- **1 Oct:** UK Black History Month
- **3 Oct:** German Unity Day
- **12 Oct:** World Health Summit
- **23 Oct:** Anniversary of 1956 Hungarian uprising
- **27 Oct:** Catalan Declaration of Independence anniversary

NOVEMBER

- **5 Nov:** Million Mask March
- **11 Nov:** Remberance Day
- **11 Nov:** Polish Independence Day
- **13 Nov:** Anniversary of the 2015 Paris terror attacks
- **21 Nov:** Ukrainian Dignity and Freedom Day
- **28 Nov:** Albanian Indepence Day

DECEMBER

- **1 Dec:** Portuguese Independence Day
- **6 Dec:** Spanish Constitution Day
- **6 Dec:** Finnish Independence Day
- **11 Dec:** Anniversary of Strasbour Christmas market attack
- **19 Dec:** Anniversary of Berlin Christmas market attack
- **20 Dec:** Anniversary of Magdeburg Christmas market attack
- **25 Dec:** Christmas

Securitas

Contact us:

For intelligence requirements: intelligence@securitas.com

For app enquiries: RIC@securitas.com