2024 Cyber-Incidents in Numbers

Period Covered by Report January 01st - December 31st, 2024

Date of the report: February 10th, 2025

SITS

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

In Focus –
2024 Cyberattack Analysis in Europe - Trends, Insights, and Projections.

The cyber threat landscape across Europe in 2024 revealed critical developments, with attacks rising in both frequency and complexity compared to 2023. This report provides a detailed analysis of attack trends, focusing on the total volume of attacks, their distribution by country and population, and the evolving dynamics of **DDoS** and **Ransomware attacks**. By exploring regional patterns, the impact of geopolitical tensions, and unique national vulnerabilities, this report aims to highlight actionable insights while projecting trends for 2025.

Special attention is given to **Ukraine** and **Israel**, whose active military conflicts are tightly interwoven with cyber threats, as well as a broader look at trends in other European countries. Finally, recommendations for businesses and organizations are offered to help them bolster their resilience in an increasingly hostile digital environment.

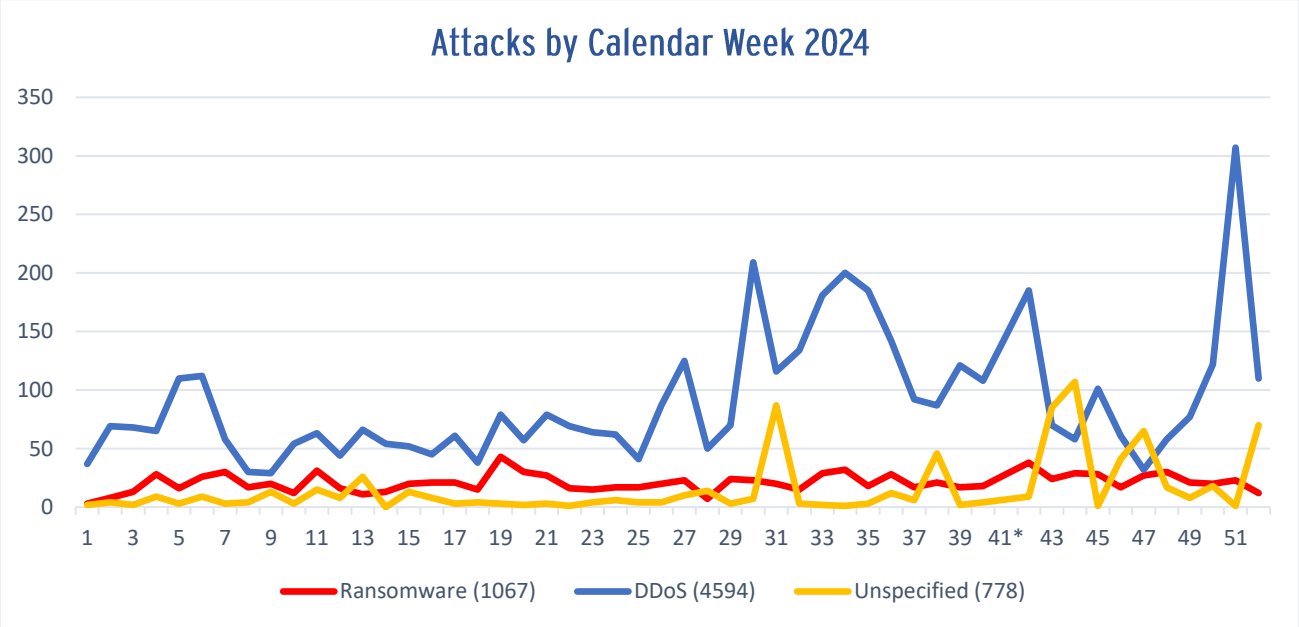

*Figure 1: depicts a line graph tracking the weekly incidence of three types of cyber threats—DDoS, ransomware, and unspecified attacks—across European countries in 2024. Each line represents one threat type, with the total occurrences. *Week 41 data is consolidated into Week 42*

1. Executive Summary of Key Findings

For cyber threat landscape across Europe in 2024 an **increase of 23.6% in cyberattacks** was observed compared to 2023. The comparison was limited to the second half of both years (weeks 26-52) due to a change in data collection methods, ensuring consistency and comparability. The total number of reported incidents rose from **3,475 to 4,295**, with **DDoS attacks** dominating (71% of all incidents) and **Ransomware** showing the fastest growth (+38.4%).

Certain countries, such as **Ukraine** and **Israel**, emerged as hotspots due to geopolitical tensions, while others, like **Luxembourg** and **Latvia**, experienced disproportionately high attack rates when adjusted for population. In contrast, larger nations such as **Germany** and **France** showed lower per capita attack rates despite high total attack counts, reflecting their large populations and stronger defensive measures.
The **top trends** observed in 2024 include:

- **DDoS attacks** peaking during high-traffic periods such as mid-year and the holiday season.
- A significant rise in **Ransomware**, particularly in high-value sectors like healthcare, finance, and energy.
- Smaller, highly digitalized countries (e.g., **Luxembourg**, **Latvia**) facing more intense attacks per capita than their larger counterparts.

A detailed company and sector-level analysis revealed that specific industries and entities were heavily targeted in 2024, with **finance** and **healthcare** being the most attacked sectors. These industries often lack the ability to tolerate downtime, making them lucrative targets for both **Ransomware and DDoS campaigns**.

Country	Ransomware	DDoS	Unspecified	All Attacks
Ukraine	6	1160	98	1264
Israel	21	292	316	629
Spain	91	424	5	520
France	116	294	55	465
United Kingdom	217	196	45	458
Germany	145	165	100	410
Czechia	14	316	42	372
Italy	126	219	19	364
Belgium	42	143	7	192
Austria	23	138	8	169
Poland	29	131	2	162
Sweden	32	92	5	129
Latvia	1	125	0	126
Finland	2	112	2	116
Romania	21	84	5	110
Switzerland	34	42	32	108
Denmark	13	92	0	105
Moldova	0	100	1	101
Netherlands	40	35	3	78
Russia	2	54	12	68
Lithuania	3	60	3	66

Luxembourg	5	59	2	66
Slovenia	1	61	0	62
Greece	10	36	1	47
Turkey	12	20	2	34
Norway	16	14	0	30

Table 1: presents a tabulated summary of cyber-attacks of top 26 European countries attacled for the year 2024, categorized by type: ransomware, DDoS, unspecified, and the total number of attacks for each country.

2. Cyberattack Developments in Europe

a. A Year of Growth - Comparing 2024

The data clearly indicates a significant rise in cyberattacks across Europe in 2024. When analyzing the latter half of the year, the total number of reported attacks increased from **3,475 attacks in 2023** to **4,295 attacks in 2024**, representing a growth of **23.6%**. This growth is not only attributable to improved reporting and data collection but also reflects an actual escalation in the intensity and scope of cyber threats.

The largest portion of this increase came from **DDoS attacks**, which continued to dominate the landscape and accounted for the majority of incidents in 2024. These attacks were designed to overwhelm servers and disrupt access to critical services. **Ransomware attacks**, though fewer in absolute terms, saw the steepest growth year-on-year, increasing by **38.4%**. This highlights a shift towards financially motivated attacks targeting industries and organizations that are particularly vulnerable to disruption.

While reporting improvements may explain part of this growth, the data strongly suggests that cybercriminals are becoming more organized and opportunistic. The increase in attacks coincides with global trends, such as the growing reliance on digital infrastructure, an expanding attack surface due to remote work, and geopolitical instability.

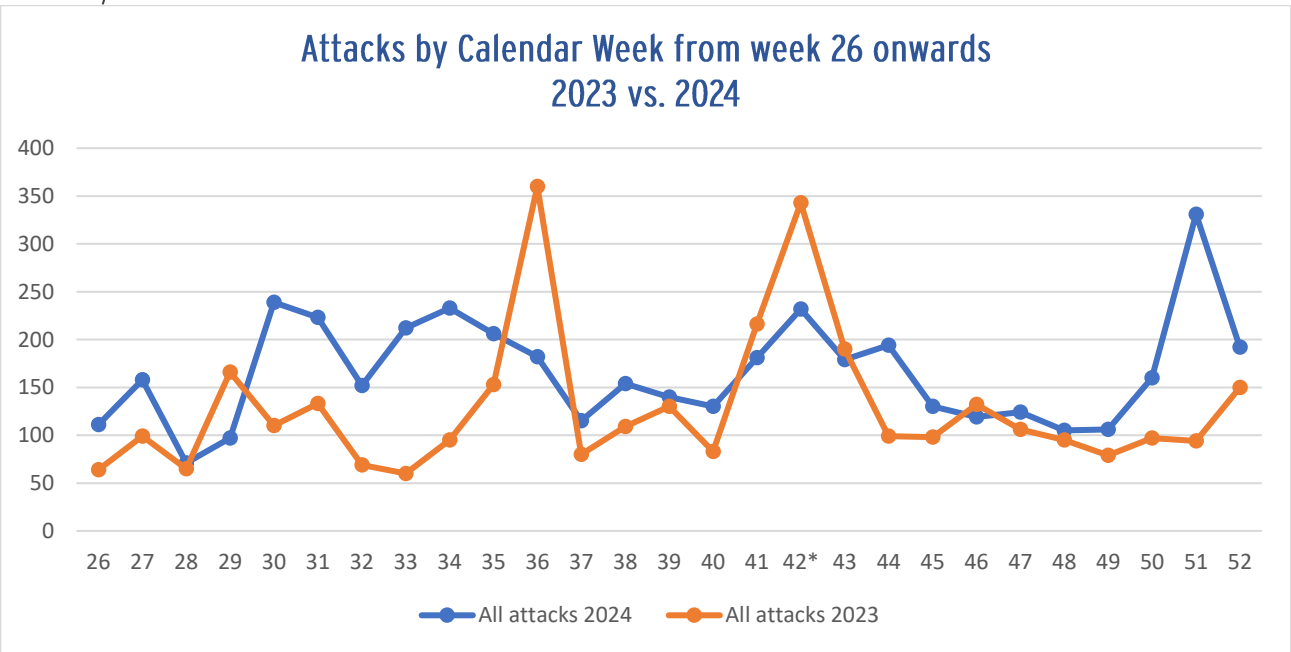

Figure 2: Shows a line graph comparing the weekly occurrence of three types of cyber threats observed across Europe in 2023 and 2024.
**Week 41 data is consolidated into Week 42*

b. Countries Most and Least Affected

The distribution of attacks across Europe in 2024 was uneven, with certain countries bearing a disproportionate burden. Ukraine stood out as the most attacked nation, experiencing **1,264 attacks** in total, followed by France (**465 attacks**) and Germany (**410 attacks**). On the other hand, Iceland and Turkey experienced the lowest attack volumes, with just **4** and **34 attacks**, respectively, underscoring how both population size and geopolitical significance influence attack patterns.

Ukraine's position as the most targeted country is unsurprising, as it remains at the center of a military conflict with Russia. Cyber campaigns against Ukraine predominantly involved **DDoS attacks** (1,160 out of 1,264 attacks), which sought to disrupt government services, critical infrastructure, and civilian systems. These cyberattacks are a direct extension of the military conflict, used to destabilize the country and pressure its allies.

Germany, despite its economic significance and technological advancement, recorded a much lower total number of attacks compared to Ukraine. The attacks in Germany were more balanced between **DDoS (165)** and **Ransomware (145)**, reflecting its role as a high-value target for both disruption and financial gain. France exhibited a similar balance of attack types, with ransomware campaigns targeting industries such as energy and healthcare, and DDoS attacks aimed at public and financial services.

At the opposite end of the spectrum, Iceland's **low attack count (4 attacks)** aligns with its small population, limited global role, and relatively low digital exposure. Similarly, Turkey's **34 attacks** suggest either underreporting or a focus on other regions by attackers. These countries are far less exposed to the types of geopolitical and economic pressures that make others high-priority targets.

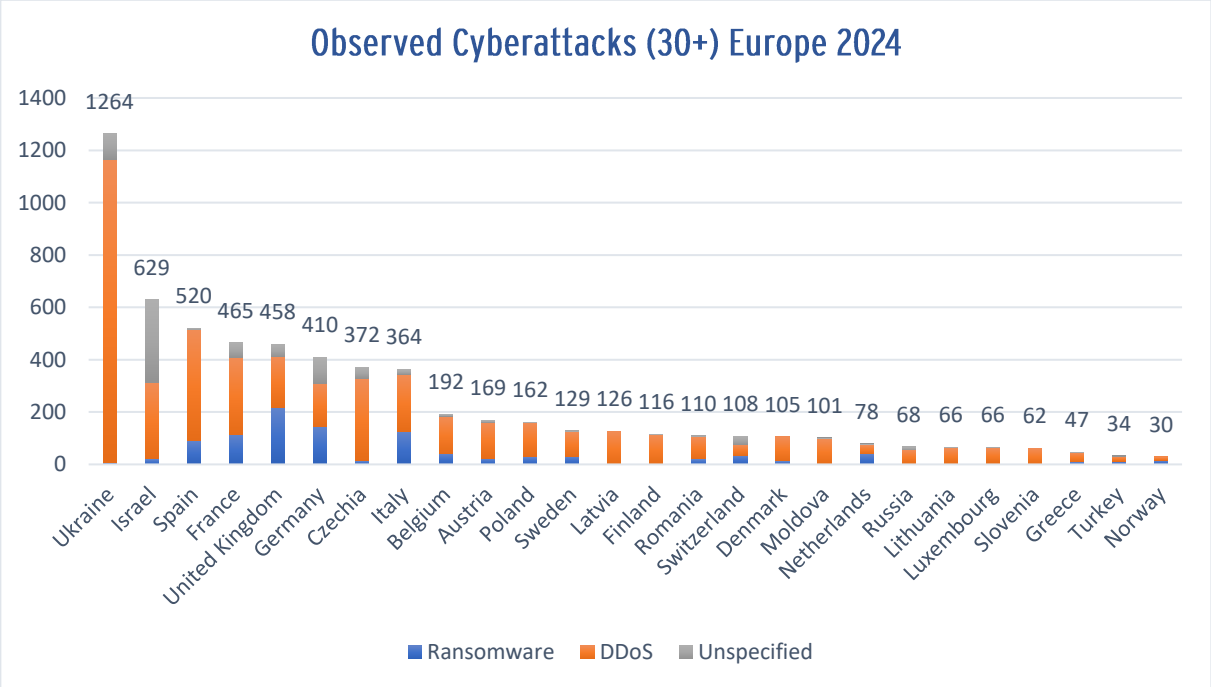

Figure 3: illustrates the distribution of cyber-attacks among the top 26 attacked European countries in 2024, with a breakdown of attack types—ransomware, DDoS, and unspecified—displayed in pie charts for each country. Total attack counts are noted above the country names.

c. Population-Adjusted Insights

When adjusting attack volumes for population size, the data paints a more nuanced picture. Smaller nations like **Luxembourg**, **Latvia**, and **Israel** emerged as the most impacted countries on a per capita basis. Luxembourg had the highest rate, with **102.74 attacks per million people**, followed by Latvia at **68.15 per million**, and Israel at **65.86 per million**.

The disproportionately high attack rate in Luxembourg reflects its status as a financial hub. With many global financial institutions and critical digital infrastructure concentrated in a small geographical area, Luxembourg is particularly susceptible to **DDoS campaigns**, which made up the majority of its attacks. **Latvia**, on the other hand, is more vulnerable to politically motivated DDoS attacks, likely linked to its proximity to Russia and broader geopolitical tensions in the Baltic region. **Israel's** high attack rate, driven largely by DDoS campaigns, underscores the intersection of its role as a technological leader and its persistent geopolitical challenges.

In contrast, larger countries like **Germany** (**4.92 attacks per million**) and **France** (**6.83 attacks per million**) appear less impacted when population is considered. This suggests that while these countries are frequently targeted, their size and resources help absorb the impact of attacks, spreading the effects over a larger population base.

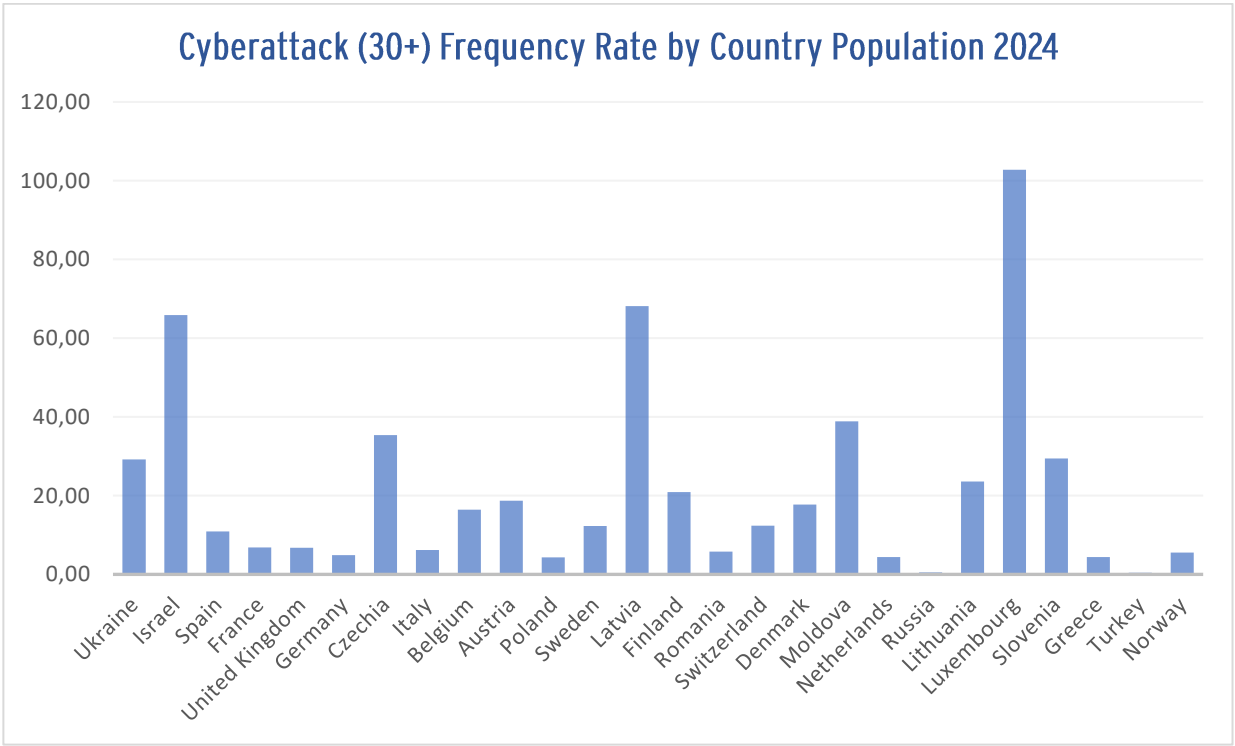

Figure 4: Displays the distribution of cyberattacks across the top 26 attacked European countries in 2024, measured per million inhabitants.

3. Regional Analysis - Ukraine, Israel, and Broader European Trends

a. Ukraine - Cyber Conflict in a War Zone

Ukraine's role as the most attacked country in Europe stems directly from its military conflict with Russia, where cyberattacks are employed as an additional theatre of war. These attacks are overwhelmingly **DDoS-focused**, with **1,160 of the 1,264 total attacks** falling under this category. The goals of these campaigns are clear:

- Disrupting government services and communication networks.
- Undermining civilian morale by targeting critical infrastructure, such as energy grids.
- Creating chaos in allied nations by targeting cross-border systems.

The sheer volume of attacks in Ukraine highlights how cyber warfare has become a fundamental component of modern conflicts. While many of these attacks may have limited lasting effects, their frequency and scale are designed to create uncertainty and pressure both domestically and internationally.

b. Israel - Persistent Targeting Amid Regional Tensions

Israel's position as one of the most attacked countries in Europe reflects its dual vulnerabilities as a technological powerhouse and a nation in a volatile region. With **292 DDoS attacks** out of a total of **629 incidents**, Israel's attackers frequently sought to overwhelm digital services critical to its tech-driven economy. These attacks often coincide with heightened political tensions in the region, suggesting a blend of state-sponsored campaigns and ideologically motivated efforts.

Ransomware, while less frequent in Israel, still posed a notable threat. Attackers likely target Israel's advanced industries and public services, viewing them as high-value opportunities for financial extortion.

c. Germany, Benelux, and Scandinavia – Regional Highlights

Germany recorded **410 total attacks**, a slight decrease from **463 in 2023**. This decline reflects improved defences, particularly against ransomware, which dropped from **169 incidents in 2023** to **145 in 2024**. However, DDoS attacks increased slightly, from **159 to 165**, targeting critical infrastructure and digital services. Despite this reduction, Germany remains a prime target due to its economic importance, with attackers focusing on manufacturing and logistics.

The Benelux region exhibited varying trends. Belgium saw a dramatic rise in attacks, increasing from **63 in 2023** to **192 in 2024**, driven by a surge in DDoS incidents, which rose from **24 to 143**. These attacks targeted government and financial services, exposing vulnerabilities in its critical infrastructure. In contrast, the Netherlands experienced a significant decline in attacks, dropping from **132 to 78**, with notable reductions in DDoS incidents from **72 to 35**, signalling the success of strengthened cybersecurity measures. Luxembourg faced a sharp increase in attacks, rising from **11 to 66**, with DDoS campaigns accounting for the majority of incidents, reflecting the country's vulnerability as a global financial hub.

Scandinavian countries displayed mixed trends. Sweden recorded **129 attacks**, down from **233 in 2023**, mainly due to a substantial decline in DDoS activity. However, ransomware incidents rose from **20 to 32**, affecting critical sectors such as healthcare and public services. Finland saw its total attacks increase from **93 to 116**, primarily due to a rise in DDoS incidents targeting digital infrastructure. Denmark experienced a similar trend, with attacks increasing from **72 to 105**, driven by DDoS campaigns targeting logistics and public services. Iceland remained largely unaffected, with only **4 total attacks** in both 2023 and 2024.

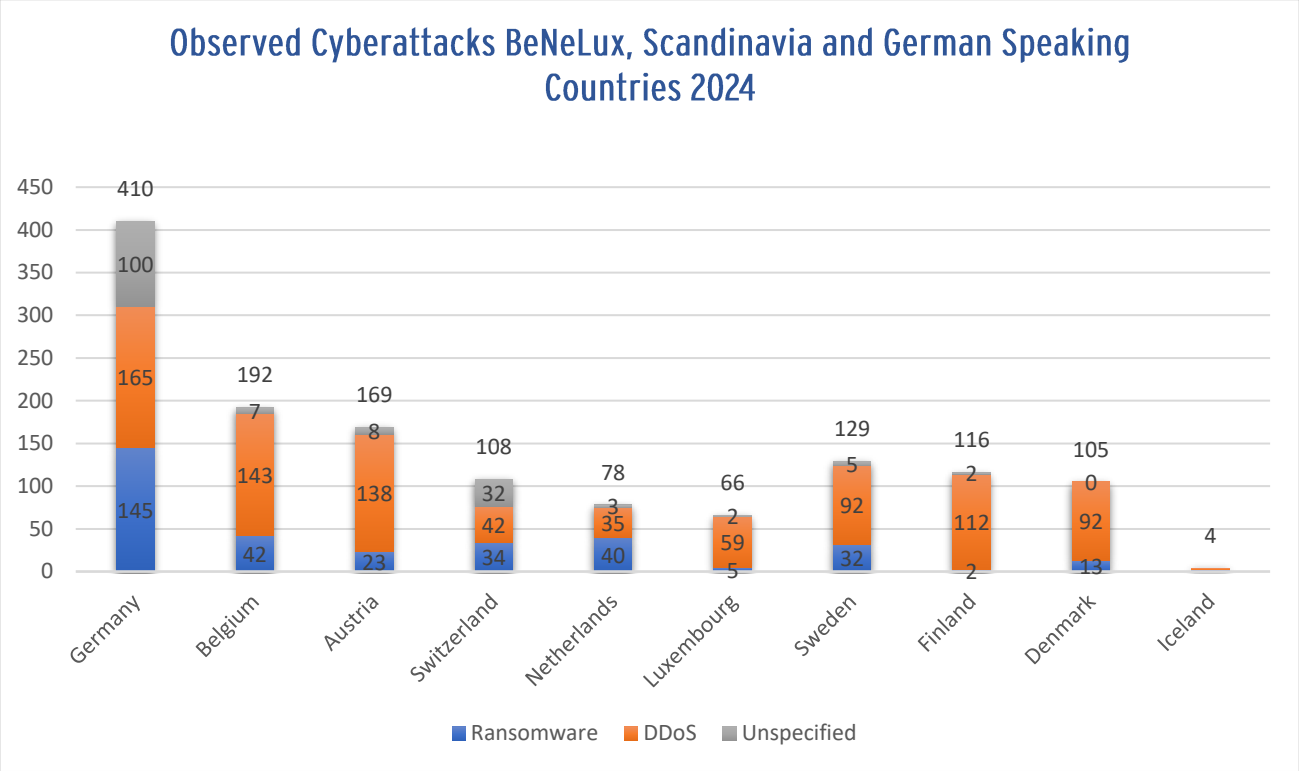

Figure 5: Shows the distribution of cyberattacks in 2024 among German-speaking countries, Benelux countries, and Scandinavia, with a breakdown of attack types–ransomware, DDoS, and unspecified–and total attack counts noted above the country names.

d. National Trends

United Kingdom – The UK reported 217 ransomware attacks, a figure that represents nearly half of its total recorded cyber incidents (458). This disproportionate focus on ransomware highlights the vulnerability of high-value sectors such as healthcare, finance, and critical infrastructure, which are especially prominent in the UK. Attackers likely perceive the UK's advanced economy and dense urban centres as lucrative targets, exploiting the country's reliance on digital infrastructure and its lower tolerance for service disruptions. Additionally, the UK's strategic geopolitical position may make it a testing ground for sophisticated ransomware campaigns.

Spain – In contrast, Spain experienced a strikingly higher number of DDoS attacks relative to ransomware. With 424 DDoS incidents, constituting over 80% of its total attacks (520), Spain stands out as a primary target for disruption campaigns. This focus is attributed to Spain's critical public services and tourism-dependent industries, both of which were frequently targeted during high-traffic periods. Cybercriminals appear to exploit seasonal surges in digital activity, leveraging DDoS attacks to create maximum disruption.

e. The Rest of Europe

Beyond the previously highlighted countries and regions, much of Europe experienced moderate attack volumes and patterns reflective of their economic and geopolitical contexts. In Eastern Europe, countries like **Latvia**, **Poland**, and **Czechia** experienced higher-than-expected DDoS volumes, with Latvia standing out as a top target on a per capita basis. These trends suggest ongoing tensions in the region and a focus on disrupting smaller, more vulnerable nations.

4. Projections for 2025

The trends observed in 2024 suggest a continued rise in cyberattacks across Europe, with an estimated growth of **10%** in total incidents. The underlying dynamics are unlikely to change significantly, with **DDoS campaigns** remaining the most common type of attack and **Ransomware** continuing to grow as attackers refine their extortion tactics.

In **Eastern Europe**, nations like Ukraine, Latvia, and Poland are expected to remain high-priority targets due to their geopolitical context. Similarly, **Israel** will likely continue to face persistent targeting, particularly during periods of heightened tension.

For **Western Europe**, nations like Germany and France are projected to see balanced attack profiles, while smaller countries like Luxembourg may experience disproportionately high DDoS activity. Meanwhile, **Southern Europe**, including Italy and Spain, will likely face an uptick in ransomware incidents targeting tourism and public services.

5. Recommendations for Organizations

Organizations across Europe must prepare for an increasingly complex and hostile cyber landscape. To improve resilience against future attacks, businesses and public institutions should prioritize the following:

1. **Defending Against DDoS Attacks**: Organizations should invest in scalable solutions capable of handling large-volume attacks, such as traffic monitoring tools and cloud-based mitigation services.
2. **Strengthening Ransomware Preparedness**: Regularly updating systems, training employees to recognize phishing attempts, and maintaining secure data backups can minimize the impact of ransomware.
3. **Developing Incident Response Plans**: Businesses should have clear procedures in place to respond to attacks, ensuring minimal disruption to operations.
4. **Focusing on High-Risk Sectors**: Industries such as finance, healthcare, and energy must adopt tailored defenses to protect against their unique vulnerabilities.

The analysis of 2024 underscores the need for vigilance in addressing the growing threats facing Europe's digital infrastructure. While countries like Ukraine and Israel grapple with the intersection of physical and cyber conflicts, the broader European landscape continues to evolve, requiring constant adaptation and investment in security measures.

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

About **AV-TEST**

AV-TEST is part of SITS Deutschland GmbH, it is an independent supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software and its use in comprehensive comparative testing of security products.

Due to the timeliness of the testing data, malware can instantly be analyzed and categorized, trends within virus development can be detected early, and IT-security solutions can be tested and certified. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, special interest magazines to publish research data, and end users to make good product choices.

AV-TEST has operated out of Magdeburg (Germany) since 2004 and employs more than 30 team members, professionals with extensive practical experience.

The AV-TEST laboratories include 300 client and server systems, where more than 2,500 terabytes of independently-collected test data, containing both malicious and harmless sample information, are stored and processed.

For more information please visit our website at https://www.av-test.org .

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org