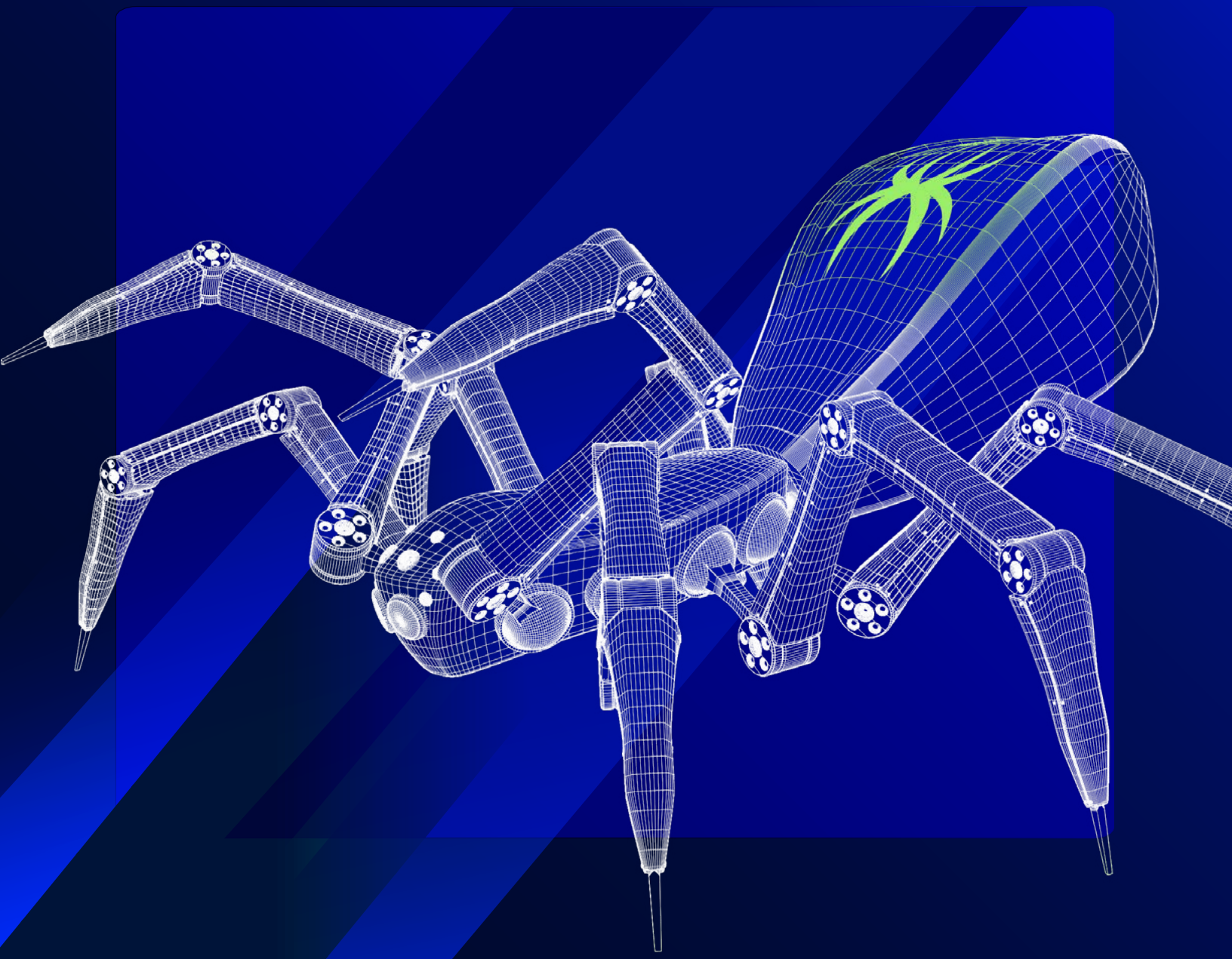
LevelBlue
SpiderLabs

How Cyberwarfare Is Reshaping the Connected World



LevelBlue SpiderLabs

Table of Contents

Executive Summary 1

The Changing Nature of Cyberwarfare 2

- Cyber Operations Become Part of Military Planning 2
- Espionage and the Value of Persistent Access 3
- Exploiting Trusted Services Rather Than Breaking Their Security 5
- Information Manipulation and Psychological Pressure 6
- The Growing Role of Automation and Artificial Intelligence 7
- Attribution and the Difficulty of Distinguishing Cyberwarfare from Cybercrime 7

When Everyday Infrastructure Becomes a Target 9

The Growing Threat to Food Preservation 10

When Missiles Meet Servers 11

- The Gulf Data Center Strikes 11
- The Russia–Ukraine War Named Data Centers as Valuable Targets 12
- Commercial Platforms and Logistics Under Physical Attack 13
- A New Dimension of Digital Resilience 13

Conclusions 15

Remediation 16

- Identify Critical Systems and Their Dependencies 16
- Eliminate Unnecessary Exposure and Secure Remote Access 17
- Strengthen Identity Security and Privileged Access 17
- Improve Detection of Suspicious Behavior 18
- Address Supply Chain and Shared Infrastructure Risks 18
- Prepare for the Loss of Entire Facilities or Regions 19
- Protect Trusted Communications and Emergency Information 19
- Maintain Safe Operations During a Cyber Incident 20
- Exercise Crisis Response and Strengthen Cooperation 20
- Priorities for Implementation 21

Appendix A: Major Incidents at a Glance 22

Appendix B: October 2025 to November 2026 Spotted Cyberwarfare Incidents 24

- October to December 2025 25
  - Around October 1 to 2, 2025: Shamir Medical Center, Israel 25
  - October 2025: Intrusion into a Quebec Municipal Water Treatment Plant 25
  - October 15, 2025: Theft of F5 BIG-IP Source Code by a State Actor 26
  - October 23, 2025 (Disclosure): Lazarus Targets European Drone Makers 26
  - November 13, 2025 (Disclosure): Espionage Run Largely by an AI Agent 27
  - November 2025 to March 2026: Sandworm Wipers in Ukraine 27
  - November 17 to 18, 2025: DoS Attacks During Danish Local Elections 28

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Table of Contents

November 27, 2025: Theft from the Upbit Exchange 28
December 11, 2025 (Disclosure): Hamas-linked Espionage Continues After the Gaza Ceasefire 29
December 12, 2025: Germany Blames Russian Military Intelligence for an Air Traffic Control Hack 29
December 13 to 14, 2025: Cyber Incident at PDVSA, Venezuela 29
December 22, 2025 to January 1, 2026: La Poste and La Banque Postale Knocked Offline 30
December 29, 2025: Destructive Attack on Polish Energy Sites (Rank 1) 30
December 29 to 30, 2025: Intrusion Attempts During Chinese Drills Around Taiwan 31
January to February 2026 32
January 2, 2026 (Disclosure): Transparent Tribe Targets India 32
January 3, 2026: US Cyber and Space Effects in the Caracas Raid (Rank 6) 32
Early January 2026: Mustang Panda Uses the Maduro Capture as Bait 33
January 8 to 28, 2026: Iran Cuts the Internet During Protests (Context) 33
January 19, 2026: UK Warning About Russia-aligned Hacktivists (Advisory) 33
January 2026: Dust Specter Targets Iraq's Foreign Ministry 34
Late January 2026: UK Links Salt Typhoon to Phone Spying on Officials 34
January 27 to February 1, 2026: APT28 Uses a New Office Flaw Against Ukraine 35
February 6, 2026: Norway Confirms Salt Typhoon Intrusions 35
February 9, 2026 (Disclosure): UNC3886 Removed from All Four Singapore Telecom Operators (Rank 8) 35
February 2026: UNC2814 Steals Email from Costa Rica's ICE, Part of a 42-country Campaign 36
February 19, 2026: Philippine Military Describes Chinese Attacks (Statement) 36
February 20, 2026: Ukrainian Hackers Claim Access to Russian Drone Operators 37
February 23, 2026: Ukraine Says Russian Intrusions Now Guide Missile Strikes on Energy (Rank 9) 37
February 25, 2026: Handala Claims a Breach of Clalit, Israel's Largest Health Fund (Unconfirmed) 37
February 28 to March 2026: The Start of the Iran War 38
February 28: US Cyber and Space Effects at the Start of the Strikes (Rank 2) 38
February 28 to March 2: Iranian App, News Sites, and TV Hijacked (Part of Rank 2) 38
February 28 to May 26: Iran's Wartime Internet Blackout (Context) 39
From February 28: A Wave of Hacktivist Claims 39
January 14 and from February 28: Hijacked Cameras Used for Reconnaissance (Rank 11) 39
March 1: Fake Rocket-alert App Spreads Spyware in Israel 40
March 1: Pakistani News Channels Hijacked 40
March 2: Attempt to Spoil Jordan's Wheat Reserve (Rank 10) 41

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Table of Contents

March 9 (Disclosure): Russia Takes Over Officials' Signal and WhatsApp Accounts (Part of Rank 14) 41
March 9 to 10: Destructive Intrusion Into the Albanian Parliament (Rank 7) 41
March 11: Stryker's Computers Wiped Worldwide (Rank 5) 42
March 11: False Missile Warnings on Israeli Station Screens 42
Before March 12: Blocked Intrusion at Poland's Nuclear Research Centre 43
March 18 (Disclosure): DarkSword iPhone Exploit Used Against Ukrainians and Others 43
March 19: US Seizes Handala and Homeland Justice Websites 43
Late February to March 24: Attacks Around Denmark's Snap Election 44
March 27: Handala Leaks Old Emails of the FBI Director 44
February to April (Reported in July): Tracking of US Personnel's Phones 44
March 31: North Korean Hijack of the Axios Software Package 45
Late March: Ransomware at a North Dakota Water Plant (Criminal Comparison) 45

April to June 2026 46
April 1: Drift Protocol Drained of About $285 Million 46
From March (Advisory April 7, Updated July 22): Iranian-affiliated Tampering with US Industrial Controllers (Rank 3) 46
April 7: FBI Takes Down a Russian Network of Hijacked Home Routers 47
April 15: Sweden Names a Failed Attack on a Power Plant 47
April 18: KelpDAO Loses About $292 Million 48
May 11 to 12: Mass Text Messages to Israelis in the Name of Iranian Intelligence 48
May 19: Europol Removes More than 14,200 Posts and Accounts Tied to the IRGC 48
May 22 (Disclosure): 600,000 Lithuanian Property Records Stolen 49
June 13 and 23: Card and Banking Outages at Iranian State Banks (Rank 15) 49
June 24 to 25: Ukraine's Postal App Knocked Out 49
June 25 to 26 (Disclosure): Turla's New Backdoor Against Ukraine 50
June 29: Israel Reports a Threefold Rise in Hostile Cyber Incidents 50

July to August 2026 51
July 2 Onward: Russian Strikes on Kyiv's Internet Infrastructure (Context) 51
Early July (Confirmed August 13): AI Agents Used Against Taiwan's Government (Part of Rank 12) 51
July (Reported August 23): Small UK Generator Shut Down for Four Days 52
July 13: EU and UK Sanction Russian Cyber Actors Together 52
July 23: Russian Group Steals Email Through a Zimbra Flaw 52
July 23: Intrusion at Saint-Noël Drinking Water Station, Quebec 53
July 26 to August: The Wave Against US Water Utilities (Rank 4) 53
August 10 to 11: Ukrainian Intelligence Claims an Attack on Wildberries 55
From May (Disclosed August 11): Fake Job Interviews for Ukrainian IT Staff 55
August 19: US Advisory on Attacks Against Siemens Controllers 55

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Table of Contents

February to August (Disclosed August 20): Russian Phishing Aimed at Officials, Academics, and Defense Staff (Part of Rank 14) 56
Criminal Cases in the Same Period 56
September to November 2026 57
September 8 (Disclosure): Sandworm Uses Google's Gemini Against Ukraine 57
September 15: UK, US, and the Netherlands Expose Iranian Spyware 57
September 2025 to July 2026 (Disclosed early October): Chinese Backdoor in Asian Governments 57
October 1: Microsoft's Annual Threat Report Puts Israel Second Among Targets 58
October 8 (Disclosure): Russian-aligned Malware in Ukrainian Industry 58
October 8: FBI Seizes Tools of a Chinese Government Contractor 59
From October 6: DoS Attack on a St. Petersburg Internet Provider 59
October 9 to 14: Ukrainian Drones Hit Russian Data Centers (Context) 59
October 13: Attack on More than 100 Azerbaijani Government Websites 60
Late August to October 15: BeyondTrust Zero-day Used by a Chinese Group (Part of Rank 13) 60
October 21 to 22: Taiwan Reports More Chinese Cyber Pressure Before Local Elections 61
October 19 to 23 (Disclosed in late October): Breach of Moldovan Government Services 61
October 22 (Disclosure): Iran's Prince of Persia Group Spies on Dissidents from US Servers 62
October 23 to 24: Palo Alto Firewalls Rooted with a Custom Exploit 62
October 24 to 27: Iranian Pressure Around Israel's General Election 63
October 28 (Disclosure): First Belarus-aligned Destructive Attack in Ukraine 64
October 28 (Disclosure): Volt Typhoon's Silent Train Relay Network 64
October 28 to 29 (Disclosure): VMware Logging Flaw Used as a Zero-day 65
October 29: About $6.3 Billion Stolen from Binance 65
October 29 (Disclosure): Suspected Hack of Freezers at US Military Commissaries 67
October 31 to November 1: Claimed Destructive Attack on Rosstat 67
November 1: False Nuclear and Chemical Alerts Through Ukraine's Air Alert App 68
November 1 to 3: Attacks on Supermarket Refrigeration Controllers Across Europe 68
November 2 (Disclosed November 3 to 4): Supplier-linked Attack Affects French Blood Service Refrigeration 69
November 2: False Alerts Through Russia's Emergency Warnings App 70
November 4: Kyiv Independent Website and Newsletter Hijacked 70
November 4 to 5 (Disclosure): Midnight Blizzard Plants Phone Exploits on Ukrainian and European Websites 71

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Table of Contents

Appendix C: The Main Conflicts in Brief **72**
- Russia and Ukraine 73
- The United States, Israel, and Iran 73
- Israel and Hamas 73
- China, Taiwan, and the Wider Indo-Pacific 74
- North Korea 74

Appendix D: Patterns: Actors, Actions, and Ways of Working **75**
- By Operator 76
- By Type of Action 77
- Ways of Working 78

Appendix E: Claims That Are Still Unproven **79**

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Executive Summary

Cyber operations have become an increasingly visible part of geopolitical conflicts, extending their impact well beyond military and government targets. Developments throughout 2025 and 2026 demonstrate how cyber capabilities are being used to support military operations, gather intelligence, disrupt essential services, and exert pressure on civilian populations.

The December 2025 attacks against Polish energy infrastructure demonstrated the potential for destructive interference with industrial control systems, while the US publicly acknowledged using cyber capabilities to disrupt Iranian communications and sensors during the opening military strikes in February 2026. At the same time, attacks affecting commercial organizations, including Stryker, and water utilities in the US highlighted how geopolitical tensions and weaknesses in critical infrastructure can translate into operational disruption, financial losses, and wider economic consequences. Not every such incident has a proven connection to a state or conflict, making reliable attribution an important part of understanding the threat.

The most significant development is not necessarily the emergence of new attack techniques, but the expanding objectives and operational roles of familiar ones. Credential theft, phishing, and the exploitation of exposed systems and malicious software remain widely used. However, these methods are increasingly combined with persistent espionage, intelligence collection supporting military activity, interference with physical processes, and manipulation of trusted communications. The November 2026 compromises of emergency-warning applications in Ukraine and Russia, which distributed false nuclear and chemical threat alerts, illustrate how attackers can undermine public confidence without causing physical destruction. Meanwhile, increased abuse of legitimate cloud services, remote-access infrastructure, and connected devices makes malicious activity harder to distinguish from normal operations. Artificial intelligence is also accelerating reconnaissance and the development of offensive tools, although its role in fully autonomous attacks remains less established than some public claims suggest.

Looking toward 2027, the principal concern is the growing dependence of governments and businesses on interconnected systems whose disruption can have consequences far beyond the initially compromised network. State-sponsored espionage, politically motivated attacks, and financially driven cybercrime increasingly overlap in their methods, even when their objectives and operators differ. These developments reinforce the importance of protecting identities, securing external access, monitoring industrial environments, and understanding dependencies on suppliers and shared infrastructure. Above all, recent incidents demonstrate that cybersecurity can no longer be measured only by an organization's ability to prevent unauthorized access. Its resilience increasingly depends on detecting interference early, limiting operational damage, and maintaining essential services when systems or trusted communications become unavailable.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

The Changing Nature of Cyberwarfare

Cyber operations have become an established part of modern geopolitical confrontation, serving military, intelligence, and political objectives alongside conventional forms of conflict. Their use is not new, but developments throughout 2025 and 2026 have made their integration into military planning more visible. Governments increasingly acknowledge cyber capabilities as part of their operations, while security researchers continue to document campaigns that combine intelligence collection, persistent network access, information manipulation and disruption.

These developments should not be mistaken for a fundamental change in how most cyberattacks are conducted. Phishing, credential theft, exploitation of known vulnerabilities, malicious software and compromised network equipment remain widely used. The more significant changes concern how these methods are combined, the objectives they support and the speed at which operations can be carried out.

Cyber Operations Become Part of Military Planning

One of the clearest developments is the increasingly visible coordination between cyber capabilities and conventional military operations. Cyber activity can help prepare the operating environment, interfere with communications, provide intelligence about potential targets, and support the assessment of military strikes.

During the opening US military operations against Iran on February 28, 2026, cyber capabilities were employed alongside conventional forces. On March 2, General Dan Caine, Chairman of the US Joint Chiefs of Staff, publicly described coordinated cyber and space operations that disrupted Iranian communications and sensor networks. According to his account, these activities were among the first elements of the military campaign, helping reduce Iran's ability to observe, coordinate, and respond to the strikes. The specific technical methods and the full extent of their effects were not publicly disclosed.

The conflict also demonstrated how commercially available surveillance equipment can acquire military significance. It was observed that Iran-linked operators intensified attempts to compromise internet-connected cameras in Israel, the Gulf states, and nearby territories beginning on February 28. The timing and geographical concentration of this activity were consistent with potential reconnaissance and battle damage assessment during missile operations. However, researchers did not establish that a particular camera compromise directly contributed to an individual strike.

Similar relationships between intelligence gathering and physical military operations have been reported during the Russia–Ukraine war, where information about infrastructure, operational conditions, and recovery activities can assist military planning.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

These developments expand the role of cyber capabilities in military operations. An intrusion does not necessarily need to destroy equipment or interrupt services to achieve a military objective. Information obtained from compromised networks or connected devices may help identify targets, assess damage, or improve situational awareness.

Espionage and the Value of Persistent Access

Cyberespionage remains one of the most consistent features of state-sponsored activity. Governments seek access to communications, military information, diplomatic correspondence, industrial research, and other data that can provide strategic advantages. In many operations, maintaining access without detection is more valuable than causing immediate disruption.

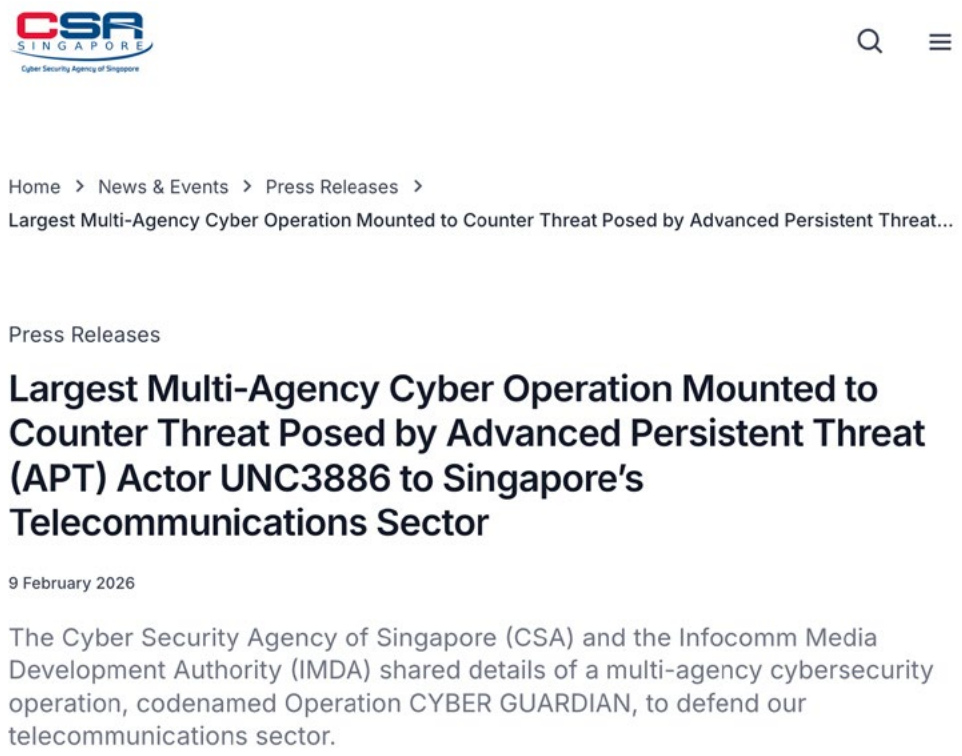


Figure 1. Statement on countering an APT threat on the Cyber Security Agency (CSA) Singapore website.

The campaign against Singapore's telecommunications sector illustrates this approach. In February 2026, Singaporean authorities disclosed further details of a coordinated response to UNC3886, an advanced threat group that had targeted all four major national telecommunications operators. Investigators identified sophisticated exploitation techniques and tools intended to conceal the attackers' presence. In one instance, access was obtained to a limited number of critical systems, but authorities found no evidence that the attackers had reached a position from which they could disrupt telecommunications services. They also reported no evidence of sensitive customer data theft.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

The operation demonstrated the strategic importance of telecommunications infrastructure. Persistent access to such networks may provide opportunities to collect intelligence and understand communications environments over extended periods. However, the presence of an advanced threat actor does not by itself establish that destructive operations were planned.



Figure 2. FBI's public statement regarding Russian General Staff Main Intelligence Directorate (GRU)'s exploitation of vulnerable routers across the world to steal critical information.

Another example emerged in April 2026, when the US Department of Justice and FBI announced the disruption of a network of compromised small office and home routers operated by a unit of Russia's military intelligence service, the GRU. The attackers had exploited known vulnerabilities and modified router settings to redirect internet traffic through infrastructure under their control, supporting the interception of credentials and sensitive communications.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

These campaigns reveal the continuing importance of infrastructure that is often overlooked in traditional security assessments. Routers, telecommunications equipment, and other network devices can provide valuable intelligence access without requiring attackers to compromise every computer or account within an organization.

Exploiting Trusted Services Rather Than Breaking Their Security

An important development in recent espionage campaigns is the growing emphasis on abusing legitimate functions of widely used digital services.

In March 2026, Dutch intelligence agencies warned that Russian state-linked operators were targeting Signal and WhatsApp accounts belonging to government officials, military personnel, and other individuals of intelligence interest. Instead of breaking the applications' encryption, attackers impersonated support personnel, persuaded users to disclose verification codes, and abused legitimate device-linking features.

The distinction matters because these operations did not depend on defeating the cryptographic protections of either platform. Attackers instead exploited the way users interact with authentication and account management systems.

Similar risks arise across cloud applications, identity services, and remote management platforms. A compromised session, unauthorized application permission, or additional trusted device may allow an attacker to operate through legitimate services. The resulting activity can be difficult to distinguish from ordinary authorized access.

This is not an entirely new technique. Social engineering and account compromise have been part of espionage for decades. What has changed is the number of services and devices connected to modern identities, as well as the amount of sensitive information accessible through a single compromised account.

For defenders, the implication is that detecting malicious behavior increasingly requires more than identifying known malware or suspicious files. Authentication events, device registrations, application permissions, and unusual patterns of access have become important sources of evidence.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Information Manipulation and Psychological Pressure

Cyber operations are also being used to influence public perception, interfere with trusted communications, and create uncertainty during periods of conflict.

During the February 2026 military strikes against Iran, attackers compromised the popular BadeSaba prayer application and several Iranian news websites. Users received messages encouraging military personnel to surrender or abandon their positions. The activity shows how a trusted civilian application could be used to distribute politically motivated messages during a military operation. The operators responsible for the compromises were not conclusively identified.

In March 2026, attackers impersonated Israel's Red Alert rocket warning application to distribute Android spyware through fraudulent SMS messages claiming to originate from the Israeli Home Front Command. The malicious application displayed genuine alerts while secretly collecting personal information, including messages, contacts and location data. Researchers identified possible links to the Hamas-associated Arid Viper group, although attribution remains unconfirmed. The campaign exploited public trust in emergency-warning services, with no evidence that the official alerting infrastructure was compromised.

A further example emerged on November 1 and 2, when emergency warning applications in Ukraine and Russia were separately compromised. Ukrainian users received false notifications concerning nuclear and chemical threats, missile attacks, and fighting in residential areas. Russia's emergency services reported that a supplementary warning application had also distributed false messages about nuclear attacks.

Authorities in both countries issued corrections and directed residents toward alternative official information channels. The responsible operators and any connection between the two incidents remain unconfirmed.

These cases illustrate a form of cyber activity in which the principal objective may be to influence behavior or undermine confidence rather than destroy a system. A false warning distributed through a trusted application can create confusion, distract public authorities, or weaken confidence in future notifications.

The immediate public reaction does not necessarily indicate that such an operation achieved its intended psychological effect. Nevertheless, compromising trusted communication channels introduces risks that conventional measures of system availability or data loss do not adequately capture.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

The Growing Role of Automation and Artificial Intelligence

Automation is increasingly influencing how cyber operations are prepared and conducted. Tools capable of identifying exposed systems, processing stolen information, and repeating technical tasks have existed for many years, but recent advances in artificial intelligence are making more complex workflows easier to automate.

In September 2026, Google Threat Intelligence Group published research describing how threat actors had progressed from using generative AI for individual tasks toward more extensive automated operations. The researchers documented an incident in which attackers compromised a cloud resource and developed an AI-assisted credential-harvesting operation in less than six hours. They also observed attempts to manipulate AI coding assistants and security analysis tools during software supply chain compromises.

State-linked groups have separately been observed using AI services for reconnaissance, scripting, social engineering, and the development of malicious capabilities. These uses suggest that AI can reduce the time required to prepare operations, adapt existing techniques, and process large quantities of information.

However, the available evidence does not support the conclusion that autonomous AI systems have replaced human operators in state-sponsored cyberwarfare. The greatest documented change is the increasing automation of individual activities and the reduction of manual effort. Human direction remains important in selecting targets, determining strategic objectives, and interpreting intelligence.

The concern is that attackers may be able to carry out familiar operations more quickly and at greater scale. Shorter intervals between reconnaissance, initial access, and subsequent activity can reduce the time available to identify and contain an intrusion.

Attribution and the Difficulty of Distinguishing Cyberwarfare from Cybercrime

The growing involvement of state agencies, politically motivated groups, and criminal operators has made the classification of cyber incidents increasingly difficult.

The same techniques used in espionage and military-related operations are also employed by financially motivated criminals. Distributed denial-of-service (DdoS), website compromises, credential theft, destructive malware can serve political, economic, or personal objectives. The method alone rarely reveals the attacker's motivation.

Hacktivist groups may claim responsibility for operations supporting one side of a conflict, while state-linked operators may use infrastructure and tools resembling those associated with ordinary criminal activity. Public claims can exaggerate the consequences of an attack, and technical indicators may not be sufficient to establish who directed an operation.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

These distinctions are important for evaluating developments in cyberwarfare. An attack occurring during a regional conflict does not necessarily form part of that conflict, while a confirmed compromise of strategically important infrastructure does not automatically demonstrate plans for sabotage.

Assessments should therefore distinguish the observed technical activity, its confirmed consequences, the evidence supporting attribution, and the strength of any connection to a geopolitical objective.

This is particularly important when analyzing incidents affecting civilian organizations, where politically motivated attacks and ordinary cybercrime may produce similar consequences but require different conclusions about the actors involved.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

When Everyday Infrastructure Becomes a Target

Much of the infrastructure that supports everyday life now depends on remotely managed digital systems. Water pumps, wastewater facilities, supermarket refrigeration, grain storage, and local electricity generation all rely on connected equipment to maintain safe operating conditions. These systems were often designed to improve efficiency, reduce maintenance costs and allow technicians to manage equipment without visiting every site. The same connectivity, however, can expose essential physical processes to unauthorized interference.

The consequences are different from those of a conventional corporate data breach. A compromised office computer may expose information or interrupt business activity. Interference with a water treatment system, refrigeration controller, or an industrial pump can affect the availability and safety of services on which people depend.

The threat became increasingly visible during 2025 and 2026. In October 2025, Canada's Cyber Centre observed incidents involving industrial control systems, including one in which attackers manipulated water pressure controls at a municipal facility, causing limited disruption to service delivery. On March 2, 2026, Jordanian authorities reported stopping an attempted intrusion into the country's grain silo management systems. According to Jordan's National Cybersecurity Center, the attackers sought to change wheat storage temperatures and damage strategic food reserves. The attempt was blocked before any operational harm occurred.

A more extensive series of incidents emerged in the United States during July 2026. The FBI and Environmental Protection Agency (EPA) warned that attackers were accessing internet-facing industrial controllers used by water and wastewater utilities. Incidents were reported in at least seven states, including a campaign affecting more than 30 municipal systems in Minnesota. Attackers changed network configurations and passwords, preventing operators from communicating with equipment and, in some cases, forcing facilities to continue operating manually. Federal authorities confirmed that some incidents degraded water operations, while CISA reported boil-water advisories and prolonged manual operation at affected utilities. The campaign has not been conclusively attributed to a particular state or group.

These attacks illustrate how small municipal utilities can be attractive targets. Their equipment is geographically distributed, often managed through cellular connections and sometimes maintained by external contractors. A single compromised controller may not affect an entire regional water network, but it can interrupt local supply, reduce pressure, disrupt wastewater handling, or require emergency intervention. More serious interference could create public health and environmental risks, although confirmed contamination or widespread injury should not be inferred from the incidents reported so far.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

The Growing Threat to Food Preservation

The latest developments in Europe have brought similar concerns into the retail sector. Between October 11 and 12, 2026, attackers interfered with refrigeration systems at hundreds of French supermarkets. By manipulating temperature and defrost settings, they caused refrigeration equipment to warm far beyond safe storage conditions. Some stores reported temperatures reaching approximately 50°C (122°F), with damage to equipment, substantial food losses and disruption to ordinary operations.

The attacks did not end in France. On November 2, a second wave affected supermarkets and other food businesses across several European countries, including Belgium, Sweden, Ireland, Luxembourg, the Netherlands and Estonia. Additional incidents or suspicious equipment failures were reported elsewhere, including Finland, Italy and Portugal. Some stores were forced to discard entire refrigerated inventories. British authorities also assisted affected food suppliers, although the publicly reported impact in the United Kingdom was limited.

The equipment involved included connected refrigeration management systems from Danfoss and other manufacturers. Investigations and technical warnings pointed to exposed management interfaces, outdated products, weak authentication and systems that were insufficiently isolated from the public internet. In some stores, refrigeration equipment was maintained by external contractors, leaving business owners with limited visibility into how their installations were connected or secured.

The French incidents alone were estimated by contemporary reporting to have caused losses running into tens of millions of euros. At the population level, the principal concerns include food availability, disruption to local suppliers and the possibility of unsafe products entering the market if temperature failures go unnoticed. The disposal of affected food reduces that health risk but creates additional economic losses and waste.

No reliable public attribution has established who conducted the European refrigeration attacks. Their timing and scale make them relevant to the wider discussion of threats against civilian infrastructure, but they should not be presented as confirmed state-sponsored cyberwarfare.

The broader significance is that equipment once considered a minor technical component can now become the point at which a cyber intrusion causes physical and financial harm. Water utilities, small power generators, cold-storage facilities, and grain-management systems share a common problem: their operational importance is often much greater than the security attention they receive.

These incidents reinforce an important lesson. Protecting essential services requires more than securing the corporate network. Organizations must understand the connected equipment on which their physical operations depend, control remote maintenance access, and ensure that operators can identify unsafe changes and recover control before a technical compromise becomes a public safety problem.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

When Missiles Meet Servers

Cyberwarfare is usually understood as the use of digital capabilities to compromise or disrupt an adversary's systems. Recent conflicts have demonstrated the reverse relationship: conventional weapons are increasingly being used against the physical infrastructure that makes digital services possible.

Data centers, telecommunications facilities, server infrastructure, and logistics platforms have become important economic assets. Some also support military and government operations. As a result, infrastructure that was previously considered primarily commercial is increasingly exposed to the physical consequences of armed conflict.

The targeting of commercial logistics infrastructure was already visible in Ukraine during 2025. On August 28, a Russian missile strike damaged a Nova Post sorting facility in Kyiv and injured three employees. The company reported delivery delays, although parcels at that facility were not damaged. In January 2026, further Russian strikes destroyed a Nova Post cargo terminal near Kharkiv, damaged its postal operations and killed four employees. Nova Post described the facility as civilian infrastructure used to distribute food, medicines, humanitarian aid, and ordinary commercial goods.

These incidents demonstrated how physical attacks against modern logistics facilities can interrupt services that depend on sophisticated digital sorting, inventory management, and distribution networks. The harm does not come from compromising software. It comes from destroying the infrastructure, equipment, and workforce needed to keep those services functioning.

The Gulf Data Center Strikes

A particularly significant development occurred on March 1, 2026, when Iranian drone strikes damaged Amazon Web Services infrastructure in the United Arab Emirates and Bahrain. AWS confirmed that two facilities in the UAE were directly struck, while a nearby strike physically damaged infrastructure at a facility in Bahrain.

The attacks caused structural damage, power interruptions, and additional damage associated with fire-suppression operations. Cloud services became unavailable or degraded, affecting businesses dependent on the regional infrastructure. Customers were advised to migrate workloads to unaffected regions and restore services using available backups.

The consequences continued long after the initial strikes. Additional disruption affected AWS infrastructure in Bahrain during April, and by September the company acknowledged that it could not restore access to some resources and data hosted exclusively in the affected region. The damage exceeded the resilience limits of the regional systems involved.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

This is an important development in the relationship between conventional warfare and commercial technology. Cloud infrastructure is designed with redundancy to withstand many equipment failures, but physical attacks against multiple facilities can overwhelm arrangements intended to provide continuous service.

The incident also challenged the assumption that data stored in a major international cloud platform is automatically protected from regional conflict. The underlying facilities remain physical assets, dependent on electricity, cooling, communications, and geographical security.

The Russia–Ukraine War Named Data Centers as Valuable Targets

The physical targeting of digital infrastructure became increasingly visible in the Russia–Ukraine conflict during September and October 2026.

On September 23, Russian strikes damaged data centers and telecommunications infrastructure in Kyiv, contributing to connectivity problems affecting approximately 100,000 households in the city and surrounding region. United DC subsequently confirmed that its long-established Kyiv data center had been effectively destroyed. The company began transferring recoverable equipment and customer services to facilities elsewhere in Europe.

Further attacks damaged Ukrainian telecommunications and data infrastructure. In October, a ballistic strike destroyed a Datagroup data center in Kyiv, with the operator reporting that the affected equipment could not be restored. Other facilities and telecommunications providers experienced damage, service interruptions, and emergency recovery operations.

Ukraine also expanded physical attacks against Russian digital infrastructure. In October, drone strikes damaged data centers operated by Yandex and other major Russian technology companies. Yandex confirmed attacks against facilities in the Ryazan and Kaluga regions, including interruptions to its computing infrastructure. Subsequent reporting described additional damage affecting banking, cloud computing and other digital services.

These attacks proved the strategic importance of computing capacity, especially when it supports financial transactions, communications, artificial intelligence development and commercial platforms. Damage to a data center may interrupt thousands of businesses or services that have no direct connection to the military operation responsible for the strike.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Commercial Platforms and Logistics Under Physical Attack

The expansion of physical attacks against commercial infrastructure was not limited to data centers. From July 2026, Ukrainian drone strikes increasingly targeted warehouses belonging to Russian e-commerce operators, particularly Wildberries and later Ozon. By late August, Reuters had documented attacks against more than 20 warehouse facilities, with approximately 1.9 million square meters (about 20.5 million square feet) of warehouse space severely damaged by fire. The consequences included destroyed inventories, disrupted delivery networks, financial losses and harm to employees and businesses relying on the platforms.

Russian attacks also caused substantial damage to Ukrainian retail and logistics operations. In September, the United Nations Human Rights Monitoring Mission reported 32 attacks during August against facilities belonging to six major Ukrainian food, retail and logistics companies, compared with 11 in July. The affected companies included supermarket operators, retailers and delivery services. The destruction of warehouses and distribution centers contributed to temporary shortages of certain food products.

The effects extend to consumers, smaller suppliers, independent businesses and employees. When a large distribution facility is destroyed, an online marketplace may remain accessible while goods cannot be stored, transported or delivered. The digital service survives, but its physical operating network does not.

Other conflicts reveal related vulnerabilities. In Sudan, in early November, drone strikes against electrical substations disrupted electricity supplies needed by water systems, hospitals, food businesses, and other essential services. These incidents should not be classified automatically as cyber operations, but they illustrate how damage to supporting infrastructure can disable services on which modern digital systems depend.

A New Dimension of Digital Resilience

Firewalls, endpoint protection, and access controls may prevent unauthorized digital access, but they cannot stop a missile from destroying a server facility or a drone strike from interrupting regional electricity supplies.

The protection of digital services during armed conflict therefore depends on a combination of cybersecurity, physical security, infrastructure redundancy, geographic distribution and recovery planning.

The developments of 2026 show that digital infrastructure has become an important part of economic and strategic competition during conflicts. Computing facilities, telecommunications networks, and logistics systems can be valuable to military operations while simultaneously supporting millions of civilian users. Their destruction can produce consequences far greater than the physical damage of the strike itself.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

This does not mean that every damaged commercial facility was deliberately selected for its digital significance. Intent must be assessed separately from confirmed damage, and the civilian or military status of a facility cannot be inferred simply from the services it provides.

The practical lesson is clear. Protecting digital operations requires understanding where the underlying infrastructure is located, how it is supplied with power and connectivity, and whether essential services can survive the physical loss of an entire facility or region.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Conclusions

The developments of 2025 and 2026 demonstrate how cyberwarfare has become increasingly integrated into geopolitical conflicts, extending beyond military and government networks into civilian infrastructure, commercial operations, and essential digital services. Cyber capabilities now support conventional military operations, intelligence gathering, industrial disruption, and information manipulation. At the same time, physical attacks against data centers, telecommunications, and logistics infrastructure have exposed the growing vulnerability of the digital economy.

The most significant change lies in the expanding objectives and consequences of established attack techniques. Credential theft, phishing, exploitation of exposed systems and malicious software remain common, but their use increasingly extends to military reconnaissance, and interference with physical processes. Incidents involving energy, water, and refrigeration systems have shown how weaknesses in connected equipment can cause wider operational and economic damage. Automation and artificial intelligence are further increasing the speed and scale of offensive activity.

These developments also highlight the importance of distinguishing confirmed incidents from suspected state involvement, attempted disruption and unverified claims. Not every cyberattack occurring during a conflict constitutes cyberwarfare, and reliable attribution remains essential to understanding the nature and significance of these operations.

Organizations must move beyond protecting individual networks toward strengthening operational resilience, detecting interference early and maintaining essential services during disruption. The defining challenge for the coming years will be not only preventing cyberattacks, but limiting their consequences before technical incidents develop into wider economic, operational, or societal crises.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Remediation

Protecting organizations against geopolitical cyber threats requires more than preventing unauthorized access to corporate networks. Attackers have exploited exposed industrial controllers, compromised legitimate accounts, interfered with trusted communications, and disrupted the infrastructure supporting essential services. At the same time, physical attacks against data centers and telecommunications facilities have shown that even well-protected digital systems can become unavailable when their supporting infrastructure is damaged.

These risks cannot be eliminated entirely, nor can organizations reliably predict when geopolitical tensions will lead to increased cyber activity. The most effective response is to reduce opportunities for compromise while strengthening the ability to detect interference, contain damage and maintain essential operations. The following measures should be prioritized according to an organization's operational dependencies, geographic exposure, and potential consequences of disruption.

Identify Critical Systems and Their Dependencies

Organizations should begin by identifying the systems and services whose loss would cause the greatest operational, financial, or public safety consequences. This assessment must extend beyond conventional IT infrastructure to include industrial controllers, building management systems, refrigeration equipment, remote maintenance connections, telecommunications services, and external technology providers.

Particular attention should be paid to smaller installations and equipment managed by contractors. Recent incidents have demonstrated that undocumented cellular modems, legacy controllers, and poorly understood remote connections can expose systems that operators believe are adequately protected.

An accurate asset inventory should identify each system's purpose, network connectivity, responsible owner, software support status and operational dependencies. Critical services should also have defined recovery objectives, including how long they can remain unavailable and how much data loss the organization can tolerate.

The objective is to understand not only what could be compromised, but also which business processes would fail as a result.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Eliminate Unnecessary Exposure and Secure Remote Access

Reducing the external attack surface remains one of the most effective defensive measures. Industrial controllers, management interfaces, engineering workstations and other sensitive equipment should not be directly accessible from the public internet unless there is an exceptional, documented operational requirement.

Remote access should be provided through controlled gateways with strong authentication, restricted permissions, centralized logging and clearly defined access periods. Connections used by equipment manufacturers, maintenance contractors, and system integrators require the same oversight as internally managed accounts.

Network segmentation should prevent a compromise in ordinary business systems from providing unrestricted access to industrial environments or other critical assets. Communication between network segments should be limited to approved systems, protocols and operational requirements.

Organizations should also review obsolete and unsupported equipment. Where immediate replacement is impractical, additional isolation, access restrictions, and monitoring should be introduced until a safe migration is possible.

Changes to operational technology must be coordinated with engineering and safety personnel. Disconnecting equipment or deploying security controls without understanding their operational consequences can itself interrupt essential services.

Strengthen Identity Security and Privileged Access

Compromised credentials and legitimate authentication mechanisms remain important entry points for both criminal and state-sponsored operations. Organizations should prioritize phishing-resistant multifactor authentication for privileged accounts, remote access, cloud administration, and other high-risk services.

Administrative privileges should be limited to approved responsibilities and activated only when required. Shared accounts, unnecessary standing privileges, and dormant external-access credentials should be eliminated wherever possible.

Protection must also extend beyond passwords. Security teams should monitor unusual session activity, unauthorized device registrations, changes to authentication settings, suspicious application permissions, and attempts to establish persistent access through trusted cloud services.

Supplier accounts deserve particular attention because attackers may exploit legitimate third-party access to enter environments that would otherwise be difficult to compromise. All external access should have an accountable owner, a documented business purpose, and an effective method of immediate revocation.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Improve Detection of Suspicious Behavior

Traditional malware signatures and known indicators of compromise remain useful, but they are insufficient against attackers using legitimate administration tools, compromised accounts or previously unseen software.

Organizations should prioritize behavioral monitoring capable of identifying network reconnaissance, repeated authentication failures, unusual administrative sessions, unexpected remote connections, and suspicious movement between systems. Endpoint and network telemetry should be correlated so that isolated events can be evaluated as part of a broader sequence of activity.

In industrial environments, detection should also cover unauthorized controller configuration changes, unexpected engineering access, modifications to control logic, changes in operating modes, and loss of communication with monitored devices. Critical configurations should be compared against verified, approved versions.

Monitoring must be adapted to operational safety requirements. Passive network observation and carefully planned integrity checks are generally preferable to intrusive scanning of sensitive equipment.

The effectiveness of these controls should be tested through authorized security assessments and controlled adversary simulations. The objective is not simply to confirm that an alert can be generated, but to establish whether the security team can recognize, investigate, and contain realistic malicious activity before it causes operational damage.

Address Supply Chain and Shared Infrastructure Risks

An organization’s resilience is increasingly dependent on the security and availability of external providers. Cloud platforms, managed service providers, equipment manufacturers, logistics partners, and telecommunications operators may all become points of failure during a cyber incident or regional conflict.

Critical suppliers should be assessed according to the consequences of their failure, not only the sensitivity of information they process. Organizations should establish which services depend on each provider, what alternative arrangements exist, and whether the supplier can continue operating during a major disruption.

Contracts should define security responsibilities, access restrictions, incident notification requirements, recovery expectations, and cooperation during investigations. Organizations should also maintain the ability to disable supplier access quickly without unnecessarily interrupting essential operations.

Where multiple facilities rely on identical equipment, software, or maintenance arrangements, security teams should consider whether a shared weakness could affect several locations simultaneously. This is particularly important for distributed energy installations, municipal infrastructure, retail refrigeration, and other remotely managed operational systems.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Prepare for the Loss of Entire Facilities or Regions

Recent physical attacks against data centers, telecommunications infrastructure, and logistics facilities demonstrate that conventional cybersecurity measures cannot guarantee service availability. Organizations must therefore account for scenarios in which infrastructure becomes inaccessible or is physically destroyed.

Critical data, configurations, and operational records should be backed up using protected, independently accessible storage. Backup strategies should include offline or immutable copies, with restoration procedures tested regularly.

For industrial systems, recovery planning must also cover controller configurations, approved control logic, engineering software, firmware, network settings and the specialized equipment required to restore operations. Backups should be checked for integrity before they are used to recover a potentially compromised system.

Organizations with significant geographic exposure should evaluate whether critical services require infrastructure in separate regions or facilities. Geographic redundancy should reflect realistic business and regulatory requirements rather than being adopted without assessing cost and complexity. Where appropriate, recovery arrangements should reduce dependence on the same power, telecommunications, and physical locations.

Most importantly, recovery exercises should demonstrate that complete business services can be restored, rather than merely proving that individual servers or files can be recovered.

Protect Trusted Communications and Emergency Information

The compromise of emergency-warning applications and other trusted communication channels has shown that information integrity is an important element of operational resilience.

Organizations responsible for public notifications, emergency alerts, or critical customer communications should apply stronger controls to the systems used to create and distribute messages. These should include restricted publishing privileges, phishing-resistant authentication, monitoring of administrative changes, and independent approval of high-impact notifications where operationally appropriate.

Emergency communication plans should provide alternative, independently controlled channels for verifying urgent information. Employees, customers, and operational personnel should know where to obtain reliable instructions if the primary website, messaging platform or notification service becomes unavailable or compromised.

Response procedures should also address the circulation of fraudulent announcements. Rapid verification and consistent communication can help contain confusion and reduce the consequences of misleading information.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Maintain Safe Operations During a Cyber Incident

Business continuity plans should account for situations in which systems are technically available but can no longer be trusted. A compromised industrial controller, manipulated monitoring display, or unauthorized configuration change may require operators to stop relying on automated functions until the integrity of the system has been established.

Organizations operating physical infrastructure should identify which essential processes can continue safely under manual or reduced-function operation. These procedures must be documented, supported by trained personnel and exercised under controlled conditions.

Clear decision-making authority is equally important. Operational and security teams should know who can isolate a network segment, disable remote access, suspend a production process, or authorize the restoration of affected equipment.

These decisions should be guided by predefined safety and business priorities. In industrial environments, an uncoordinated technical response can create consequences as serious as the original intrusion.

Exercise Crisis Response and Strengthen Cooperation

Cybersecurity preparation should involve senior management, operational personnel, legal teams, communications staff, and external service providers, not only IT and security specialists.

Organizations should conduct realistic exercises involving scenarios such as a compromised supplier, simultaneous disruption of multiple facilities, loss of regional cloud infrastructure, or manipulation of official communications. Exercises should evaluate both technical response and management decisions, including escalation, customer communication, regulatory notification, and the continuation of essential services.

Incident response plans should establish how evidence is preserved, how affected systems are isolated, and how information is shared with relevant national cybersecurity authorities, sector regulators and trusted industry partners.

During periods of heightened geopolitical tension, threat intelligence should be used to identify relevant changes in attacker behavior and adjust monitoring priorities. However, defensive decisions should remain grounded in observed technical activity and organizational exposure rather than unverified claims of responsibility.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Priorities for Implementation

Organizations should begin with the measures capable of reducing immediate exposure: identifying critical assets, removing unnecessary internet access, securing privileged accounts, reviewing third-party connections, and verifying that protected backups are available.

The next priority should be improving monitoring and incident readiness, particularly around authentication, remote administration, network discovery, and unauthorized changes to critical systems. These measures should be followed by realistic recovery exercises, supplier resilience assessments, and improvements to geographic or operational redundancy where justified.

Progress should be measured through verifiable outcomes. Organizations should know how many critical assets remain exposed, whether unauthorized access can be detected promptly, how quickly compromised privileges can be revoked, and whether essential services can be restored within agreed recovery limits.

The principal lesson from recent conflicts is that no organization can rely entirely on preventing compromise. Effective defense requires reducing the opportunities available to attackers, identifying interference before it spreads, and preserving the ability to operate when systems, suppliers, or infrastructure fail. Cybersecurity investment should ultimately be measured by its contribution to operational resilience, public safety, and the continuity of essential services.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Appendix A: Major Incidents at a Glance

The ranking weighs the real or potential effect, how directly the incident served a military or strategic campaign, and how well it is documented. Each incident is described in full in Appendix B.



LevelBlue SpiderLabs

Rank	Incident	Date	Where	Actor (basis)
1	Destructive attack on Polish wind, solar and heat and power plants	Dec. 29, 2025	Poland	Russia-linked (CERT Polska, ESET)
2	US cyber effects at the start of the Iran war; Iranian app and TV hijacks	Feb. 28 to March 2, 2026	Iran	US (self-acknowledged); hijacks unclaimed
3	Iranian-affiliated tampering with US industrial controllers	From March 2026	United States	Iranian-affiliated (FBI-led advisory)
4	Summer wave against US water utilities	July 26 to August 2026	United States	Not attributed
5	Stryker global wiper attack	March 11, 2026	United States, global	Handala, MOIS persona (US DOJ)
6	Cyber and space effects in the Caracas raid	Jan. 3, 2026	Venezuela	US (self-acknowledged)
7	Destructive intrusion into the Albanian Parliament	March 9 to 10, 2026	Albania	Homeland Justice, MOIS-linked (US DOJ, AKSK)
8	UNC3886 removed from all four Singapore telecom operators	Disclosed Feb. 9, 2026	Singapore	China-nexus (Mandiant)
9	Russian cyber targeting of Ukrainian energy, and new wipers	Nov. 2025 to Feb. 2026	Ukraine	Russia (Ukrainian officials, ESET)
10	Attempted sabotage of Jordan's wheat silos	March 2, 2026	Jordan	Traced to Iran (Jordan NCSC)
11	Camera hijacking for wartime reconnaissance	Jan. to March 2026	Israel, Gulf, Cyprus, Lebanon	Iran-linked (Check Point)
12	AI agents running intrusion campaigns	Sept. 2025; July 2026	Global; Taiwan	Chinese state-sponsored (Anthropic); Taiwan case unattributed
13	BeyondTrust zero-day and F5 source-code theft	Oct. 2025; Aug. to Oct. 2026	Global	China-nexus (Mandiant; press for F5)
14	Russian takeover of officials' messaging and cloud accounts	March to Aug. 2026	Netherlands, Europe, Ukraine	Russian state (AIVD/ MIVD); suspected Russian (Google)
15	Card and banking outages at Iranian state banks	June 13 and 23, 2026	Iran	Unattributed; Black Wolves claimed

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Appendix B: October 2025 to November 2026

Spotted Cyberwarfare Incidents



LevelBlue SpiderLabs

October to December 2025

Around October 1 to 2, 2025: Shamir Medical Center, Israel

Evidence: Confirmed by the victim or a government. Attribution: Government (Israel National Cyber Directorate: Iran). Conflict: Iran-Israel.

Around Yom Kippur, attackers hit Shamir Medical Center (Assaf Harofeh) in Be'er Yaakov. Patient data was leaked. Officials first said the attack was blocked at an early stage; the National Cyber Directorate later said the attackers had tried, without success, to interfere with hospital operations. The Qilin ransomware group appeared to demand $700,000 to keep the data private, and Israeli authorities first blamed a Russian-speaking criminal group. On about October 22, 2025, the directorate said Iran was behind it, as part of a wave of Iran-backed attacks using stolen usernames and passwords.

Technical detail. Little has been published beyond the use of stolen credentials. Why a known ransomware brand appeared in an operation later attributed to Iran was not explained; it may have been cover, or criminal access may have been reused. No disruption to patient care was reported.

Sources: The Times of Israel | Iran International

October 2025: Intrusion into a Quebec Municipal Water Treatment Plant

Evidence: Confirmed by the victim or a government. Attribution: Government (Canada's CSE names NoName057(16)). Conflict: Russia-NATO hybrid pressure.

Canada's Communications Security Establishment said in its annual report, released at the end of June 2026, that it was told in October 2025 of a breach at a water treatment plant run by a Quebec municipality. According to the report, the intruders reached the plant network and gained access to "many crucial systems" before being caught. CSE attributes the intrusion to the pro-Russian group NoName057(16), which is better known for denial-of-service (DoS) attacks. The plant was not named, and no damage or water-safety impact was reported.

Technical detail. CSE published no technical account. Headlines saying that the attackers controlled pumps and chlorine dosing are not backed by the text of the reports. The case fits what the UK NCSC described in January 2026: Russia-aligned groups reaching industrial devices through badly secured remote-access software such as VNC.

Sources: ThreatBeat summary of the CSE report | CSE announcement of its 2025-2026 annual report

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

October 15, 2025: Theft of F5 BIG-IP Source Code by a State Actor

Evidence: Confirmed by the victim or a government. Attribution: Unknown officially; press reports point to a China-nexus group. Conflict: Strategic espionage.

F5 told the US Securities and Exchange Commission on October 15, 2025, that a "highly sophisticated nation-state threat actor" had long-term access to its product development environment and knowledge platform. F5 found the intrusion on August 9, 2025, and delayed disclosure at the request of the US Department of Justice. The attackers took part of the BIG-IP source code, information on unpublished vulnerabilities, and configuration details for a small share of customers. The same day, CISA issued Emergency Directive 26-01, ordering federal civilian agencies to inventory their BIG-IP devices, check whether management interfaces were exposed to the internet, and install F5's updates by October 22.

Technical detail. Bloomberg reported that the malware was BRICKSTORM, a backdoor associated with the China-nexus cluster UNC5221. Public analyses describe BRICKSTORM as a self-contained Linux program that communicates over WebSocket, multiplexes connections, and acts as a SOCKS proxy, hiding stolen data inside normal HTTPS traffic. The stolen vulnerability data is the real risk: F5's next quarterly release fixed 44 vulnerabilities, 27 of them rated High. No evidence was found that the source code was changed.

Sources: The Hacker News | FedRAMP on CISA ED 26-01 | Hack The Box on BRICKSTORM

October 23, 2025 (Disclosure): Lazarus Targets European Drone Makers

Evidence: Documented by credible technical research. Attribution: Researchers (ESET: Lazarus, North Korea). Conflict: Strategic; the activity began in March 2025.

ESET reported a new wave of Operation DreamJob, the long-running Lazarus scheme built on fake job offers, against European defense companies working on drones. Three were compromised: a metal engineering firm, an aircraft parts maker, and a defense contractor. ESET thinks the aim was drone know-how. The activity started in March 2025, before this period, so it is included only as a disclosure.

Technical detail. Victims received trojanized copies of a PDF reader and open-source tools (MuPDF, TightVNC, Notepad++ plugins). These loaded the ScoringMathTea remote-access trojan, which supports about 40 commands, through a chain of loaders.

Sources: ESET | Security Affairs

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

November 13, 2025 (Disclosure): Espionage Run Largely by an AI Agent

Evidence: Documented by credible technical research. Attribution: Researchers (Anthropic: Chinese state-sponsored, high confidence). Conflict: Strategic espionage.

Anthropic said it detected, in mid-September 2025, a group it calls GTG-1002 using its Claude Code tool to run an espionage campaign against about 30 organizations in technology, finance industry, and government. A small number of intrusions succeeded. Within about ten days, Anthropic banned the accounts, told the victims, and informed the authorities. Victims were not named, and the attribution is the company's own.

Technical detail. The operators built a framework in which the AI agent did an estimated 80 to 90 percent of the work, sometimes several requests per second. People chose the targets and approved key steps, such as escalating access and deciding what to take. The work was cut into small tasks that each looked like routine security testing, and the model was told it worked for a legitimate penetration-testing firm. The model often invented results, claiming passwords that did not work, so humans had to check its findings. No new exploits were written; existing tools were used.

Sources: Anthropic report (PDF) | TechTalks | National CIO Review

November 2025 to March 2026: Sandworm Wipers in Ukraine

Evidence: Documented by credible technical research. Attribution: Researchers (ESET: Sandworm, high confidence for the ZOV wiper). Conflict: Russia–Ukraine, direct.

ESET detected the ZOV wiper at a Ukrainian financial institution in November 2025; the exact date and the extent of the damage are not public. ESET's report for October 2025 to March 2026 adds that Sandworm stepped up destructive attacks over the winter, using several new wiper families against Ukrainian government and private targets. The victims were not named.

Technical detail. ZOV was pushed to individual machines by a deployment script. ESET used its code and that script as the main reference when it attributed the Polish DynoWiper attack a month later. Sandworm usually spreads wipers through Active Directory Group Policy, which requires domain administrator rights.

Sources: ESET on DynoWiper and ZOV | ESET APT Activity Report Q4 2025 to Q1 2026

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

November 17 to 18, 2025: DoS Attacks During Danish Local Elections

Evidence: Confirmed by the victim or a government. Attribution: Government (Danish Defence Intelligence Service). Conflict: Russia-NATO hybrid pressure.

On the eve of and during the November 18 local elections, DoS attacks briefly took down the websites of the Social Democrats, the Conservatives, the Red-Green Alliance and the Moderates, several government sites, and the English-language Copenhagen Post, for several hours. NoName057(16) claimed the attacks. Votes were counted by hand and were not affected. On December 18, 2025, the Danish Defence Intelligence Service said NoName057(16) and Z-Pentest have connections to the Russian state, which "uses both groups as part of its hybrid attacks against the West." It was Denmark's first public attribution of cyberattacks to Russia, and the Russian ambassador was summoned.

Technical detail. NoName057(16) runs DDoSia, a tool that pays volunteers to flood listed sites with requests. The same statement tied Z-Pentest to a December 2024 attack on the Tureby Alkestrup waterworks in Køge, where pump pressure was changed, at least three pipes burst, and about 50 households were without water for seven hours.

Sources: The Record | Euronews | Security Affairs

November 27, 2025: Theft from the Upbit Exchange

Evidence: Confirmed by the victim or a government. Attribution: Suspicion by South Korean authorities (Lazarus). Conflict: North Korean revenue.

At 04:42 Korean time on November 27, more than twenty Solana-based tokens were drained from one of the Upbit exchange's online ("hot") wallets. The operator, Dunamu, first reported a loss of 44.5 billion won, about $30 million, and later revised it to about 54 billion won as prices moved. Upbit covered the loss from its own funds. South Korean investigators suspect Lazarus; this is a suspicion, not a court finding.

Technical detail. Hundreds of transfers went out within minutes to newly created wallets. That pattern points to stolen signing keys and automated draining rather than a flaw in Solana itself. About 2.3 billion won in one token was frozen with the issuer's help.

Sources: Scorechain | The Block | NK News

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

December 11, 2025 (Disclosure): Hamas-linked Espionage Continues After the Gaza Ceasefire

Evidence: Documented by credible technical research. Attribution: Researchers (Palo Alto Networks Unit 42: Hamas-affiliated). Conflict: Israel-Hamas, regional espionage.

The Gaza ceasefire took effect on October 10, 2025. Unit 42 reported that Ashen Lepus, also known as WIRTE, kept spying on Middle Eastern government and diplomatic bodies afterward, while other Hamas-linked groups went quiet. Targets included entities in Oman, Morocco, and the Palestinian Authority, with lures suggesting new interest in Turkey. In several cases the operators took diplomatic documents by hand, once directly from an email account.

Technical detail. The new AshTag toolset starts with DLL sideloading: a renamed legitimate program loads a malicious library called AshenLoader. A modular .NET backdoor then runs its payloads in memory, which leaves less evidence on disk.

Sources: Unit 42 | The Record | L'Orient Today on the ceasefire

December 12, 2025: Germany Blames Russian Military Intelligence for an Air Traffic Control Hack

Evidence: Confirmed by the victim or a government. Attribution: Government (Germany: APT28). Conflict: Russia-NATO hybrid pressure.

Germany summoned the Russian ambassador and said it had "clear evidence" that APT28, a unit of Russian military intelligence (GRU), carried out the August 2024 cyberattack on Deutsche Flugsicherung, the state air traffic control company. It also accused Russia of running the Storm-1516 disinformation campaign around the February 2025 federal election. The attack itself predates this period; the attribution falls inside it.

Sources: The Record

December 13 to 14, 2025: Cyber Incident at PDVSA, Venezuela

Evidence: Confirmed by the victim or a government. Attribution: Unknown (Venezuela blamed the US without evidence). Conflict: Unproven; it came during the US blockade of Venezuelan oil.

Over the weekend of December 13 to 14, Venezuela's state oil company PDVSA was hit by a cyberattack. PDVSA said only administrative systems were affected and exports went on, and blamed "foreign interests" and the United States. Company sources told Reuters the opposite: "There's no delivery of cargoes, all systems are down." The incident came days after the US seized a sanctioned Venezuelan tanker.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. A PDVSA source told Reuters that ransomware had been detected days earlier and that the antivirus clean-up itself took the administrative system down. That fits criminal ransomware as easily as state sabotage. No technical evidence has been published.

Sources: Security Affairs, citing Reuters | BOE Report (Reuters)

December 22, 2025 to January 1, 2026: La Poste and La Banque Postale Knocked Offline

Evidence: Confirmed by the victim or a government. Attribution: Claim (NoName057(16)); France's DGSI investigating. Conflict: Russia-NATO hybrid pressure.

During the Christmas rush, a DoS attack took down laposte.fr, the La Banque Postale online bank and app, Digiposte, and La Poste's digital identity service. Card payments, cash machines, and post office counters kept working. La Poste said no customer data was affected and declared the attack contained on December 26, but a new wave began at 03:15 on January 1. NoName057(16) claimed it, and the domestic intelligence service DGSI took over the investigation.

Technical detail. La Poste described "several billion connection attempts per second" from "several million IP addresses" of hijacked devices. The attack came five months after Europol's Operation Eastwood took down more than 100 NoName057(16) servers, which shows how fast the volunteer network rebuilt.

Sources: La Poste | Security Affairs

December 29, 2025: Destructive Attack on Polish Energy Sites (Rank 1)

Evidence: Confirmed by the victim or a government. Attribution: Researchers (CERT Polska: The Static Tundra / Berserk Bear cluster; ESET: Sandworm, medium confidence). Conflict: Spillover of the Russia–Ukraine war onto a NATO member.

On December 29, attackers struck more than 30 wind and solar farms, a large combined heat and power (CHP) plant serving nearly half a million customers, and a manufacturing company. At the renewable sites, they cut the link between the farms and the grid operator, which lost monitoring and remote control; the farms kept generating. At the large CHP plant, they launched a wiper that endpoint protection blocked. In August 2026, CERT Polska disclosed a second, smaller CHP plant serving about 50,000 people, where the attackers stopped a steam turbine and the water treatment for the process, briefly halting cogeneration. Heat supply to customers never stopped and there was no grid outage.

Technical detail, renewable sites. The attackers got in through FortiGate devices exposed to the internet and used as VPN gateways, where some accounts could log in without multi-factor authentication (MFA). Inside the substations that connect the farms to the grid, they hit remote terminal units, protection relays, operator computers, and serial device servers made by Hitachi Energy, Mikronika, and Moxa. They uploaded corrupted firmware, deleted files, and reset devices to factory settings.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail, large CHP plant. The attackers had been inside for months. They mapped the network, took operational data and obtained privileged Active Directory accounts. On December 29, they placed DynoWiper in a shared folder and tried three times to run it through Group Policy; ESET's software blocked all three attempts. DynoWiper goes through every fixed and removable drive, skips system folders, overwrites the start of each file with random bytes (and many random points inside large files), deletes the files and restarts the machine.

Technical detail, manufacturer. Entry was through a Fortinet device whose configuration had leaked on a criminal forum. A PowerShell wiper that CERT Polska calls LazyWiper was pushed by Group Policy; CERT believes part of it was written with a large language model.

Technical detail, smaller CHP plant. The attackers first took over a wind farm's FortiGate, then a Teltonika RUTX50 cellular router, and tunneled into a private mobile network (APN) run by the grid operator. That network let any device talk to any other. From December 18, they scanned it and found a WAGO PFC200 controller still using its default web password, which gave them a way into the plant's control network. On December 25, they connected to three Siemens controllers. On December 29, between about 05:30 and 10:10, they switched Siemens S7-300, S7-1200, and S7-1500 controllers to STOP and set passwords on them, reset Moxa devices to unreachable addresses, then wiped the router, reset the FortiGate, and left the WAGO controller unable to start. No malware was used; every step used normal device functions. The operator first thought it was a contractor's mistake.

Attribution. CERT Polska found infrastructure overlapping "to a high degree" with the cluster called Static Tundra, Berserk Bear, Ghost Blizzard, or Dragonfly, which US prosecutors have previously tied to Russia's FSB. ESET attributes DynoWiper to the GRU's Sandworm with medium confidence, while saying it did not see how the attackers got in. Both point to Russia; which service did it is still disputed. In July 2026, the EU cited the attack when it sanctioned Russian cyber actors.

Sources: CERT Polska report | CERT Polska follow-up | ESET technical analysis | Elastic Security Labs | Help Net Security | The Hacker News on the APN attack

December 29 to 30, 2025: Intrusion Attempts During Chinese Drills Around Taiwan

Evidence: Documented by credible technical research. Attribution: Government (Taiwan National Security Bureau: China). Conflict: China-Taiwan.

During Chinese military exercises around Taiwan at the end of December, Taiwan's National Security Bureau counted about 2.08 million intrusion attempts against government networks on the first day and 2.09 million on the second, along with 799 suspicious social media accounts and more than 19,000 "controversial" messages. These are attempts, not confirmed breaches.

Sources: IANS

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

January to February 2026

January 2, 2026 (Disclosure): Transparent Tribe Targets India

Evidence: Documented by credible technical research. Attribution: Researchers (CYFIRMA: APT36, aligned with Pakistan). Conflict: India-Pakistan rivalry.

CYFIRMA reported a phishing campaign by Transparent Tribe, also called APT36, against Indian government, academic, and strategic organizations. It is espionage; the number of victims was not published.

Technical detail. The email carried a ZIP file with a Windows shortcut disguised as a PDF. Opening it ran mshta.exe, which pulled a remote script that loaded the spyware in memory and showed a decoy PDF. How the malware made itself persistent depended on the antivirus product it found on the machine. The final payload can control the computer, steal files, take screenshots, and read the clipboard.

Sources: The Record | The Hacker News

January 3, 2026: US Cyber and Space Effects in the Caracas Raid (Rank 6)

Evidence: Documented by credible technical research. Attribution: Self (US acknowledged its own operation). Conflict: US military operation against Venezuela.

During the raid that captured Nicolás Maduro, Gen. Caine said US Cyber Command and Space Command helped set it up by "layering different effects." Cyber Command said it was "proud to support" the operation. President Trump had said "the lights of Caracas were largely turned off due to a certain expertise we have." Venezuela's power company Corpoelec said substations around Caracas were knocked out; power came back at several of them within about two hours, and the outages were limited to the area of the operation.

Technical detail. None has been published. A former Air Force cyber officer who reviewed videos said the lights went out instantly, not in the flickering way of rolling blackouts. A former White House cyber official, Michael Daniel, noted that people on the ground switching equipment manually would look the same. Whether the blackout came from code, from people or from physical action is not established.

Sources: Axios | Nextgov

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Early January 2026: Mustang Panda Uses the Maduro Capture as Bait

Evidence: Documented by credible technical research. Attribution: Researchers (Acronis: Mustang Panda, moderate confidence). Conflict: China-US rivalry.

Within days of the raid, a China-linked group sent US government agencies and policy organizations a ZIP file named "US now deciding what's next for Venezuela.zip." Acronis linked it to Mustang Panda. It is not known whether anyone was compromised.

Technical detail. The archive used DLL sideloading to load a malicious library, kugou.dll, which installs a custom backdoor Acronis calls LOTUSLITE. It talks to a fixed server, offers a remote command shell and file operations, and restarts at every logon through a registry entry.

Sources: The Register | The Hacker News

January 8 to 28, 2026: Iran Cuts the Internet During Protests (Context)

Evidence: Confirmed by the victim or a government. Attribution: Iranian authorities. Conflict: Domestic control of information.

On January 8, the twelfth day of nationwide protests, Iran cut internet and phone services across the country. NetBlocks measured connectivity at about two percent of normal on January 16. The shutdown was eased on January 27, but most users could only reach approved sites. This is a state cutting its own networks, not a cyberattack. It is included because the same tool was used again, for much longer, during the war.

Sources: Cloudflare on Iran's shutdown | Cloudflare Q1 2026 disruption summary | IntelliNews on Cloudflare data

January 19, 2026: UK Warning About Russia-aligned Hacktivists (Advisory)

Evidence: Confirmed by the victim or a government. Attribution: Government (UK NCSC). Conflict: Russia-NATO hybrid pressure.

The NCSC warned that NoName057(16), CARR, and Z-Pentest were running constant DoS attacks on UK councils, infrastructure operators, and others because of Western support for Ukraine. It also warned that these groups reach industrial devices in water, food, farming, and energy through badly secured VNC connections. This is a warning, not a single incident, but it explains how cases like the Quebec and Danish water intrusions happen.

Sources: NCSC | Security Affairs

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

January 2026: Dust Specter Targets Iraq's Foreign Ministry

Evidence: Documented by credible technical research. Attribution: Researchers (Zscaler: linked to Iran, moderate to medium-high confidence). Conflict: Iranian regional intelligence.

Zscaler ThreatLabz saw a campaign in January 2026 against Iraqi officials, using lures in the name of Iraq's Ministry of Foreign Affairs and a hacked Iraqi government website to host malware. It links the group, which it calls Dust Specter, to Iran, with clear overlap with APT34. Zscaler's own write-up gives two slightly different confidence levels.

Technical detail. One chain starts with a password-protected archive containing a dropper disguised as WinRAR. It launches a legitimate VLC player that loads a malicious library, which runs encoded PowerShell commands every 15 seconds; a second legitimate program loads the part that talks to the command server. A second chain uses a single .NET implant that opens a fake ministry survey in Google Forms while running commands in memory. The command server checks each request, insists on a particular browser identity, shuffles its replies and reportedly accepts only victims in certain places. Emojis and placeholder values in the code suggest parts were written with generative AI.

Sources: Zscaler ThreatLabz | Security Affairs

Late January 2026: UK Links Salt Typhoon to Phone Spying on Officials

Evidence: Stated by officials or the media without technical detail. Attribution: Government acknowledgment of "a cluster of activity" (UK), with details from press reports. Conflict: China-UK strategic espionage.

On January 26 to 27, The Telegraph reported that the Chinese espionage campaign known as Salt Typhoon had accessed phones used by senior aides to three former British prime ministers, possibly since 2021, and that this was found in 2024. The UK government has spoken only of a "cluster of activity" linked to Salt Typhoon, without saying what it involved. China's foreign ministry called the claims baseless. How much of the press account is confirmed is unclear.

Sources: The Register | Militarnyi, summarizing The Telegraph

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

January 27 to February 1, 2026: APT28 Uses a New Office Flaw Against Ukraine

Evidence: Documented by credible technical research. Attribution: Government (CERT-UA: APT28). Conflict: Russia–Ukraine, direct.

Microsoft disclosed the Office flaw CVE-2026-21509 around January 26 as already being exploited. A day later a booby-trapped document called "Consultation_Topics_Ukraine(Final).doc" had been made, and on January 29, a phishing wave reached more than 60 people in Ukrainian central government bodies. CERT-UA found three more documents aimed at organizations in EU countries and blamed APT28. The number of infected computers is not public.

Technical detail. Opening the document made the computer connect to an attacker server and download a shortcut file. That dropped a library posing as a Windows component, with its code hidden inside an image. It survived reboots by hijacking a legitimate Windows component and through a scheduled task. The final payload was Covenant, an open-source attack framework, which used the legitimate Filen cloud storage service for its traffic.

Sources: The Register | The Hacker News

February 6, 2026: Norway Confirms Salt Typhoon Intrusions

Evidence: Confirmed by the victim or a government (Norway's security service, with few details). Attribution: Government (Norway's PST: Salt Typhoon). Conflict: China strategic espionage.

In its 2026 national threat assessment, Norway's Police Security Service said Salt Typhoon had broken into several Norwegian organizations by exploiting vulnerable network devices. The organizations and sectors were not named.

Sources: TechCrunch

February 9, 2026 (Disclosure): UNC3886 Removed from All Four Singapore Telecom Operators (Rank 8)

Evidence: Confirmed by the victim or a government. Attribution: Researchers (Mandiant: China-nexus); Singapore named no country. Conflict: Strategic espionage.

Singapore disclosed Operation Cyber Guardian, its largest joint cyber operation so far. For more than eleven months during 2025, hundreds of defenders from the Cyber Security Agency, the media regulator IMDA, the armed forces' Digital and Intelligence Service, GovTech, the Internal Security Department, and others worked to remove UNC3886 from the networks of M1, SIMBA Telecom, Singtel, and StarHub. Phone and internet services were never interrupted and there was no sign that customer records were taken.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. The attackers used at least one previously unknown vulnerability to get past a firewall, then installed rootkits to stay hidden. Most of their access was limited, but they took small amounts of technical data on network configuration, the sort of material that helps long-term intelligence collection. UNC3886 has been seen before exploiting zero-days in FortiGate and VMware products; officials did not say which products were involved this time.

Sources: Singapore CSA | Minister Teo's speech | Help Net Security | The Register

February 2026: UNC2814 Steals Email from Costa Rica's ICE, Part of a 42-country Campaign

Evidence: Confirmed by the victim or a government for Costa Rica; documented by credible technical research for the wider campaign. Attribution: Researchers (Google: suspected China-nexus). Conflict: Strategic espionage.

On February 25, Google's Threat Intelligence Group and Mandiant said they had disrupted UNC2814, a suspected China-nexus espionage group tracked since 2017 that mainly targets telecom operators and governments. By February 18, it had 53 confirmed victims in 42 countries, with suspected infections in at least 20 more. On March 12, Costa Rica's government said its state electricity and telecom company ICE was one of them: about 9 GB of staff email was taken. ICE said customer data and power systems were not affected, and China's embassy denied any role.

Technical detail. The backdoor, GRIDTIDE, uses a Google Sheets spreadsheet as its command channel. It writes details of the infected machine into one cell, checks another cell every second for commands, and moves files in pieces through further cells. On the Linux server Mandiant examined, it disguised itself as a system tool, moved to other machines over SSH and sent traffic out through a SoftEther VPN. That server held national ID numbers, voter IDs and phone numbers. Google did not see data leave, but believes the access could allow theft of call records and misuse of lawful interception systems. Google shut down the attackers' cloud accounts and took over their domains.

Sources: Google Threat Intelligence | Teletica | Security Affairs

February 19, 2026: Philippine Military Describes Chinese Attacks (Statement)

Evidence: Stated by officials or the media without technical detail. Attribution: Government statement (Philippine armed forces). Conflict: China-Philippines, South China Sea.

The head of the Philippine armed forces' cyber command, Brig. Gen. Joey Fontiveros, said threats from China-based state-backed actors were growing in 2026 because of the South China Sea dispute. He listed malware, denial of service, data leaks, and website defacements, and said foreign attempts to reach intelligence data had been detected but no major breach confirmed. No specific incident was described.

Sources: GMA News

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

February 20, 2026: Ukrainian Hackers Claim Access to Russian Drone Operators

Evidence: Stated by officials or the media without technical detail. Attribution: Claim (Fenix group and InformNapalm). Conflict: Russia–Ukraine, direct.

The pro-Ukrainian Fenix group and InformNapalm volunteers said they had broken into accounts of dozens of Russian servicemen and into systems used by drone operators, from mid-2025 to February 2026. They published screenshots they say show drones being relayed through Belarusian mobile towers, and they say the information was used for Ukrainian strikes. None of it has been independently verified.

Sources: Euromaidan Press | Militarnyi

February 23, 2026: Ukraine Says Russian Intrusions Now Guide Missile Strikes on Energy (Rank 9)

Evidence: Stated by officials or the media without technical detail. Attribution: Government (Ukrainian officials). Conflict: Russia–Ukraine, direct.

Oleksandr Potii, head of Ukraine's State Service of Special Communications, and Natalia Tkachuk of the National Security and Defence Council, said Russian cyberattacks on the energy sector now mostly gather intelligence for missile and drone strikes rather than causing outages directly. Intruders map facilities, follow repair crews, and measure how fast systems recover. Access is used before strikes to choose targets and afterward to judge the damage. No individual case was published.

Why it matters. Together with the Sandworm wipers above, this is the clearest official description of cyber operations feeding a cycle of physical strikes.

Sources: The Record

February 25, 2026: Handala Claims a Breach of Clalit, Israel's Largest Health Fund (Unconfirmed)

Evidence: Claim by the actor only. Attribution: Claim (Handala). Conflict: Iran-Israel.

Handala, the persona the US later tied to Iran's Ministry of Intelligence, said it had hacked Clalit Health Services and published documents with members' personal details, claiming more than 10,000 patients were affected. Clalit said it was checking whether the claim was credible, and the National Cyber Directorate was looking into it. No later confirmation from Clalit was found.

Sources: Ynet

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

February 28 to March 2026: The Start of the Iran War

The United States and Israel began strikes on Iran on February 28, 2026 (Operation Epic Fury on the US side, Roaring Lion on the Israeli side). Cyber operations ran on both sides from the first hours.

February 28: US Cyber and Space Effects at the Start of the Strikes (Rank 2)

Evidence: Documented by credible technical research. Attribution: Self (US acknowledged). Conflict: US/Israel-Iran, direct.

At a Pentagon briefing on March 2, Gen. Caine said Cyber Command and Space Command were “first movers” in the operation, “layering non-kinetic effects” that “effectively disrupted communications and sensor networks,” leaving Iran “without the ability to see, coordinate, or respond effectively.” No target was named. Israeli cyber operations were widely reported but not officially described.

Technical detail. None has been published. Reports that Israeli intelligence had long had access to Tehran’s traffic cameras and mobile networks come from press sources and have not been confirmed.

Sources: Nextgov | CSIS

February 28 to March 2: Iranian App, News Sites, and TV Hijacked (Part of Rank 2)

Evidence: Confirmed by the victim or a government. Attribution: Unknown; nobody claimed it. Conflict: US/Israel-Iran, psychological operation.

At 09:52 Tehran time on February 28, minutes after the first explosions, users of the BadeSaba prayer app (more than 5 million installs) started receiving notifications that began “Help has arrived” and urged soldiers to defect. Official news sites, among them the IRNA agency, were defaced. On March 1 to 2, hours after strikes hit the state broadcaster’s buildings, the satellite feed of Iranian TV channels was hijacked to show addresses by Benjamin Netanyahu and Donald Trump. Some outlets reported Israeli involvement, but it has not been confirmed.

Technical detail. No forensic report exists. Sending mass notifications through a real app needs access to its push service or back end, and hijacking a satellite channel needs the means to transmit to the satellite. Both suggest a capable operator rather than opportunists.

Sources: Schneier on Security, citing Wired | The Media Line | TechCrunch

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

February 28 to May 26: Iran's Wartime Internet Blackout (Context)

Evidence: Confirmed by the victim or a government. Attribution: Iranian authorities. Conflict: Wartime control of information.

Within hours of the strikes, Iran cut international connectivity. NetBlocks measured traffic at four percent of normal on February 28 and about one percent from March 6. Unit 42 reported that limited access to Iran's domestic network started coming back around April 17. On May 25, President Pezeshkian ordered international access restored, and NetBlocks saw partial restoration on May 26, about 88 days after the cut. This is not a foreign cyberattack, but it shaped the cyber war: ESET saw activity by long-established Iranian groups drop, probably because of these restrictions.

Sources: AI-Monitor | Unit 42 | ESET APT Activity Report

From February 28: A Wave of Hacktivist Claims

Evidence: Documented by credible technical research (claims documented; most effects not verified). Attribution: Claims by about 60 groups. Conflict: US/Israel-Iran.

Radware counted 149 claimed DoS attacks against 110 organizations in 16 countries in the first days of the war; three groups, Keymous+, DieNet, and NoName057(16), made about three quarters of them. Kuwait, Israel, and Jordan were hit most, and nearly half the targets were government bodies. On March 2, NoName057(16) declared solidarity with Iran and turned on Israeli party, municipal, and telecom sites. Intel 471 judged the real damage "likely negligible"; most claims were backed only by screenshots of website status checks.

Sources: The Hacker News on Radware data | Intel 471

January 14 and from February 28: Hijacked Cameras Used for Reconnaissance (Rank 11)

Evidence: Documented by credible technical research. Attribution: Researchers (Check Point: Infrastructure linked to Iran). Conflict: US/Israel-Iran, battlefield intelligence.

Check Point saw targeted probing of internet-connected Hikvision and Dahua cameras in Israel and Qatar on January 14 and 15. From February 28, the activity grew across Israel, Qatar, Bahrain, Kuwait, the UAE, and Cyprus, and on March 1, it focused on parts of Lebanon. The locations matched areas under Iranian missile and drone fire. Check Point believes the aim was live reconnaissance and checking the results of strikes.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. The attackers used old, already patched flaws: CVE-2017-7921, CVE-2021-36260, CVE-2023-6895, and CVE-2025-34067 in Hikvision devices and CVE-2021-33044 in Dahua devices, working from VPN and server infrastructure Check Point associates with Iranian actors. In the June 2025 war, a street camera near the Weizmann Institute was reportedly taken over shortly before a missile hit the area. For any single strike in 2026, the use of camera footage is an inference, not a proven fact.

Sources: Check Point Research | Security Affairs

March 1: Fake Rocket-alert App Spreads Spyware in Israel

Evidence: Documented by credible technical research. Attribution: Researchers (Acronis: possibly Arid Viper, not confirmed). Conflict: Israel's wars with Iran and Hamas.

On March 1, Israelis received text messages from senders posing as the official "Oref Alert" service, saying the warning app was faulty and needed an update. The link led to a trojanized copy of the Red Alert app. Acronis and Unit 42 both documented it.

Technical detail. The fake app pretends to come from Google Play and runs the real Red Alert app so that alerts still work. In the background it reads all text messages, contacts, device accounts, and location, lists installed apps, and can draw fake screens over other apps to steal passwords. Acronis says this fits Arid Viper, a group linked to Hamas, but also fits other Android spyware operations, so the link is possible but not proven.

Sources: Acronis | Unit 42

March 1: Pakistani News Channels Hijacked

Evidence: Confirmed by the victim or a government. Attribution: Unknown. Conflict: Unproven, during the war.

On the evening of March 1, the satellite feeds and live streams of Geo News, ARY News, and Samaa TV showed messages urging Pakistanis to turn against their armed forces. Geo said it had fought off attempts on its feed for 24 hours before the intruders got through. A group calling itself Pakistan Cyber Force then hijacked India's ABP News in retaliation. No one has been identified.

Sources: SC Media

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

March 2: Attempt to Spoil Jordan's Wheat Reserve (Rank 10)

Evidence: Confirmed by the victim or a government. Attribution: Government (Jordan's National Cybersecurity Center: traced to Iran). Conflict: US/Israel-Iran.

Jordan's National Cybersecurity Center stopped an intrusion into the silo management system of the Jordan Silos and Supply General Company. Its head, Mohammad Al-Smadi, said the goal was to change the storage temperature of the wheat to damage the national reserve, and that the attempt was traced to Iran. The system was not affected.

Technical detail. None has been published. Warmer grain spoils and attracts insects over days or weeks, so a successful change might not have been noticed quickly. Few attacks on food supply systems have ever been reported publicly.

Sources: Petra news agency

March 9 (Disclosure): Russia Takes Over Officials' Signal and WhatsApp Accounts (Part of Rank 14)

Evidence: Confirmed by the victim or a government. Attribution: Government (Dutch services AIVD and MIVD: Russian state hackers). Conflict: Russia-NATO intelligence contest.

The Dutch intelligence services warned of a Russian campaign against the Signal and WhatsApp accounts of officials, military personnel, and civil servants worldwide, and said Dutch government staff were among the victims. Once inside, the attackers could read incoming messages, including group chats.

Technical detail. No flaw in the apps was used. Victims were tricked into handing over codes and PINs, usually by a fake "Signal Support" chatbot, or into scanning a code that added the attacker's device through the apps' normal "linked devices" feature. The encryption was not broken; the attacker simply became one more device on the account.

Sources: AIVD | Malwarebytes

March 9 to 10: Destructive Intrusion Into the Albanian Parliament (Rank 7)

Evidence: Confirmed by the victim or a government. Attribution: Government (Albania's AKSK points to actors tied to Iran's Ministry of Intelligence; the US DOJ ties Homeland Justice to the same ministry). Conflict: Iran-Albania, during the war.

Attackers broke into the Albanian Parliament's network and deleted 183 virtual desktops and much of the data on a file server. The Parliament said its core systems and website kept working, and it restored from backups. Homeland Justice, the persona Iran has used against Albania since 2022, claimed the attack and published files.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. Albania's National Cyber Security Authority (AKSK) reconstructed the attack. At 03:14 on March 9, the attackers logged in to the Parliament's VPN with stolen credentials belonging to a supplier, from a server in Albania. They failed to reach a domain controller, moved through internal machines over SSH and opened a tunnel to a server in the Netherlands. Over the day they tried passwords against the VMware management system and got in as administrator at 21:42. On March 10, they downloaded the list of virtual machines, changed the administrator password and from 10:40 deleted the virtual machine files directly through the management interface. Their last access was at 11:07. The Exchange email server was not touched, contrary to the group's claim of having MPs' email; the leaked files came from a file share. AKSK suspects data was taken earlier through the MEGA cloud service and calls its attribution preliminary.

Sources: AKSK incident report (PDF) | BalkanWeb | Balkan Insight

March 11: Stryker's Computers Wiped Worldwide (Rank 5)

Evidence: Confirmed by the victim or a government. Attribution: Government (US DOJ: Handala is a front for Iran's Ministry of Intelligence). Conflict: US/Israel-Iran, Iranian retaliation.

The US medical technology company Stryker lost its internal Microsoft environment on March 11. Offices closed in dozens of countries, and order processing, manufacturing and shipping stopped; customers had to order by hand through sales staff. Stryker said its medical devices were not affected. Handala claimed it wiped more than 200,000 systems and stole 50 TB; those are its own figures. By late March, Stryker said it had largely recovered.

Technical detail. According to a source cited by BleepingComputer, the attacker took over an administrator account, created a new top-level administrator, and used the remote wipe function of Microsoft Intune, the company's device management service, to erase nearly 80,000 devices between 05:00 and 08:00 UTC. No ransomware was used. Stryker first said there was no malware; on March 23, it said, with Unit 42, that the attacker had used a malicious file "to run commands which allowed them to hide their activity" and that it "was not capable of spreading." The case shows that a device management system can be turned into a wiper without writing any wiper code.

Sources: SecurityWeek | Security Affairs | KrebsOnSecurity | US DOJ

March 11: False Missile Warnings on Israeli Station Screens

Evidence: Confirmed by the victim or a government. Attribution: Unknown. Conflict: US/Israel-Iran, psychological operation.

Advertising screens at Herzliya and Tel Aviv Shalom stations showed messages saying the stations would be hit by Iranian missiles and telling people to leave. Israel Railways said the screens belong to a private advertising company and are "not connected to the railway infrastructure." The screens were switched off and the National Cyber Directorate investigated. Iran's Fars agency falsely claimed the whole rail system had been hacked.

Sources: Calcalist | JNS

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Before March 12: Blocked Intrusion at Poland's Nuclear Research Centre

Evidence: Confirmed by the victim or a government. Attribution: Government indication (Polish minister: first signs point to Iran, possibly a false flag). Conflict: Unproven.

Poland's National Centre for Nuclear Research, which runs the MARIA research reactor, found and blocked an intrusion before any system was compromised. Digital Affairs Minister Krzysztof Gawkowski said the first entry points identified were related to Iran, while the government warned that this could be a deliberate deception. The reactor kept running at full power.

Sources: Security Affairs | Help Net Security

March 18 (Disclosure): DarkSword iPhone Exploit Used Against Ukrainians and Others

Evidence: Documented by credible technical research. Attribution: Researchers (Google: a suspected Russian group, UNC6353, among several users). Conflict: Russia–Ukraine for the Ukrainian campaign.

Google, with Lookout and iVerify, disclosed DarkSword, a complete iPhone exploit kit used since at least November 2025 by several actors: a Turkish surveillance company, PARS Defense (in Turkey and Malaysia), an actor tracked as UNC6748 (Saudi Arabia), and the suspected Russian group UNC6353, which planted it on Ukrainian websites from at least December 2025 to March 2026. After a copy leaked online, Proofpoint saw the FSB-linked group TA446 use it on March 26 in emails spoofing the Atlantic Council.

Technical detail. DarkSword is written entirely in JavaScript and chains six flaws in iOS 18.4 to 18.7, three of them previously unknown, to go from a web page to full control of the phone. UNC6353's payload, GHOSTBLADE, grabs iMessage, Telegram, and WhatsApp messages, contacts, stored passwords, Wi-Fi passwords, location history, photos, and crypto wallet data in one pass, then deletes crash reports. iOS 26.3 fixes all six flaws.

Sources: Google Threat Intelligence | Security Affairs | The Hacker News

March 19: US Seizes Handala and Homeland Justice Websites

Evidence: Confirmed by the victim or a government. Attribution: Government (US DOJ and FBI: Iran's Ministry of Intelligence). Conflict: US/Israel-Iran.

The Justice Department seized four domains (Handala-Hack.to, Handala-Redwanted.to, Justicehomeland.org, and Karmabelow80.org) and said Iran's Ministry of Intelligence and Security ran them as fake hacktivist fronts that mix destructive attacks with psychological operations. The FBI linked them through shared leak sites, Iranian IP addresses, and a common way of working. The State Department offers up to $10 million for information on Handala. The websites came back online under new addresses soon afterward.

Sources: US DOJ

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Late February to March 24: Attacks Around Denmark's Snap Election

Evidence: Documented by credible technical research. Attribution: Researchers (CSIS Denmark: the pro-Russian DDoSIA network). Conflict: Russia-NATO hybrid pressure.

After Denmark called an early election for March 24, the Danish security firm CSIS saw new DoS attack targeting of Danish and Greenlandic organizations. Around Easter, the attacks moved to transport, airports, postal, and municipal services, and in early April, to banks and energy firms. No systems were compromised, no data was taken and voting was not affected.

Sources: CSIS Denmark

March 27: Handala Leaks Old Emails of the FBI Director

Evidence: Confirmed by the victim or a government. Attribution: Government (Handala is a front for Iran's Ministry of Intelligence, per US DOJ). Conflict: US/Israel-Iran, psychological operation.

Handala published personal photos, documents, and emails from FBI Director Kash Patel's personal Gmail account, dating from before he took office. The FBI confirmed his personal email had been targeted and said the material was "historical in nature and involves no government information." Handala's claim to hold classified files is unverified.

Sources: BleepingComputer

February to April (Reported in July): Tracking of US Personnel's Phones

Evidence: Stated by officials or the media without technical detail. Attribution: Researcher assessment (Citizen Lab: partly linked to an Iranian mobile operator). Conflict: US/Israel-Iran.

In July, the Financial Times, quoting Citizen Lab researcher Gary Miller, reported attempts to locate US personnel in the region during the war through mobile network signaling and advertising data, with some requests traced to an Iranian operator. No link to any strike has been shown and the data has not been published. In September, Reuters reported that the US military was turning off advertising trackers on its devices.

Sources: Citizen Lab | Reuters via The Star

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

March 31: North Korean Hijack of the Axios Software Package

Evidence: Confirmed by the victim or a government. Attribution: Researchers (Google: UNC1069, North Korea). Conflict: North Korean revenue and access.

An attacker took over the account of a maintainer of Axios, one of the most used JavaScript libraries (more than 100 million downloads a week), and published two poisoned versions. They were available for about three hours before being removed. StepSecurity saw more than 12,000 projects contact the attacker's server.

Technical detail. An old, long-lived access token let the attacker skip the project's normal release process. The poisoned versions pulled in an extra package whose install script dropped a remote access trojan for macOS, Windows, and Linux that checked in every minute. Google linked it to UNC1069 through earlier versions of the same malware and shared infrastructure.

Sources: Tenable

Late March: Ransomware at a North Dakota Water Plant (Criminal Comparison)

Evidence: Confirmed by the victim or a government. Attribution: Unknown ransomware gang. Conflict: None established.

Ransomware hit a server connected to the control system of the Minot water treatment plant. Staff isolated it and ran the plant by hand, and the water stayed safe. It is here as a reminder that not every water sector incident in 2026 was related to nation-state actor activity.

Sources: KFYR-TV

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

April to June 2026

A two-week ceasefire between the US, Israel, and Iran, brokered by Pakistan, took effect on April 8 and was extended on April 21. The US and Iranian presidents signed the Islamabad Memorandum on June 17 to end the war, but both sides broke the truce many times, and it collapsed on July 8. Cyber activity continued throughout. (Al Jazeera · Reuters via ThePrint · Anadolu Agency · AFP via The Jakarta Post)

April 1: Drift Protocol Drained of About $285 Million

Evidence: Confirmed by the victim or a government. Attribution: Researchers (Elliptic and TRM Labs: North Korea; Drift: UNC4736, medium-high confidence). Conflict: North Korean revenue.

The Solana-based trading platform Drift lost about $280 million to $286 million (estimates differ) in minutes. No software bug was exploited. Drift says the attackers spent about six months gaining trust, posing as a trading firm, meeting contributors in person at conferences through go-betweens who were not Korean, and keeping in touch on Telegram. Drift believes two contributors were compromised through a malicious code repository and a fake wallet app.

Technical detail. The attackers collected enough approvals from Drift's security council using "durable nonces," a Solana feature that lets a signed transaction be carried out later, so the signers approved transactions without understanding what they would do. The attackers then took over administrative powers, removed the safety delay, listed a fake token that the platform's price feeds valued at hundreds of millions as collateral, and lifted the withdrawal limits. The vaults were emptied in about ten seconds. The money went through Tornado Cash and cross-chain bridges. There is no government attribution.

Sources: BleepingComputer | The Hacker News | Elliptic

From March (Advisory April 7, Updated July 22): Iranian-affiliated Tampering with US Industrial Controllers (Rank 3)

Evidence: Confirmed by the victim or a government. Attribution: Government (FBI-led advisory: actors in the CyberAv3ngers lineage, tied to the IRGC). Conflict: US/Israel-Iran, Iranian action on US soil during the war.

On April 7, the FBI, CISA, NSA, EPA, Department of Energy, and Cyber Command's Cyber National Mission Force issued joint advisory AA26-097A. Since at least March 2026, actors affiliated with Iran had accessed internet-facing Rockwell Automation controllers in US water, energy, and government facilities, causing operational disruption and financial losses at several victims, who were not named. A July 22 update added controllers from Schneider and Siemens and more indicators. Summaries of the advisory place the actors in the line of CyberAv3ngers, a group US authorities tied to the cyber unit of Iran's Revolutionary Guards; Unit 42 separately saw the same group turn to Rockwell equipment.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. No software flaw was needed. The actors looked for CompactLogix and Micro850 controllers reachable from the internet, connected with Rockwell's own engineering software using missing or default passwords, installed a small SSH server to keep access, copied the controller programs, changed them and loaded them back, and altered operator screens so staff saw false readings. The July update added a more worrying finding: at one confirmed victim, the attackers' changes disabled alarm and shutdown logic. That is a step from disruption toward a safety risk.

Sources: BleepingComputer | CISA | 1898 & Co. summary of AA26-097A | 1898 & Co. on the July update

April 7: FBI Takes Down a Russian Network of Hijacked Home Routers

Evidence: Confirmed by the victim or a government. Attribution: Government (US DOJ: GRU Unit 26165, APT28). Conflict: Russia-NATO intelligence contest.

The Justice Department announced a court-approved operation against thousands of hacked TP-Link routers worldwide, including in more than 23 US states, which the GRU unit known as APT28 had used since at least 2024. The FBI sent commands to the US routers to collect evidence, restore their normal settings, and block the attackers.

Technical detail. The GRU used known router flaws to steal passwords, then changed the routers' DNS settings so that lookups went to servers it controlled. For chosen targets it returned fake addresses for look-alike sites, including Outlook web mail, to capture passwords, login tokens, and email. Ordinary users were left alone, which kept the network quiet.

Sources: US DOJ

April 15: Sweden Names a Failed Attack on a Power Plant

Evidence: Confirmed by the victim or a government. Attribution: Government (Sweden: A pro-Russian group with links to Russian intelligence). Conflict: Russia-NATO hybrid pressure.

Sweden's Minister for Civil Defence, Carl-Oskar Bohlin, said a pro-Russian group with ties to Russian intelligence tried a destructive cyberattack on a Swedish thermal power plant in early 2025, and that a built-in protection stopped it. Neither the plant nor the group was named. The attack predates the period; the attribution does not.

Sources: TechCrunch

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

April 18: KelpDAO Loses About $292 Million

Evidence: Confirmed by the victim or a government. Attribution: Researchers (LayerZero, preliminary, and TRM Labs: TraderTraitor, part of Lazarus). Conflict: North Korean revenue.

On April 18, KelpDAO reported suspicious cross-chain activity involving its rsETH token and froze the contracts. About 116,500 rsETH, worth roughly $292 million, had been taken. TRM Labs counted it, with Drift, as the two largest thefts of 2026 so far, and estimated that North Korean groups had stolen about $577 million in January to April, 76 percent of all crypto hack losses in that period, and about $643 million by mid-year.

Technical detail. According to early analysis, the attackers went after the service that checks KelpDAO's cross-chain messages on the LayerZero network. They took over several of the data nodes it relied on, fed them false blockchain data, and flooded the honest nodes so the checker used the poisoned ones. A fake message then passed as genuine and released the tokens. The money went through Tornado Cash. The attribution is preliminary.

Sources: Hackmag | The Block on TRM Labs figures | NK News on mid-year figures

May 11 to 12: Mass Text Messages to Israelis in the Name of Iranian Intelligence

Evidence: Confirmed by the victim or a government. Attribution: Unknown formally; the messages invoke Iran, and Israel's cyber directorate was investigating. Conflict: Influence and recruitment.

Overnight, many Israelis received text messages from senders with names like "IntelOp." Some invited them to "cooperate in the field of intelligence" with Iran, others offered to buy videos of the war, or repeated earlier threats. The National Cyber Directorate said the aim was to manipulate people, collect personal data, and hurt morale, and that it was trying to find the source. Phones were not hacked.

Sources: Israel Hayom

May 19: Europol Removes More than 14,200 Posts and Accounts Tied to the IRGC

Evidence: Confirmed by the victim or a government. Attribution: Government (Europol: IRGC). Conflict: Wartime propaganda.

Between February 13 and April 28, Europol's Internet Referral Unit and authorities from 19 countries removed or restricted more than 14,200 posts, accounts, and links tied to Iran's Revolutionary Guards, including their main X account with over 150,000 followers. The content mixed political messaging with martyrdom themes and AI-generated videos calling for revenge, in six languages.

Sources: Maryland Coordination and Analysis Center, reproducing the Europol release

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

May 22 (Disclosure): 600,000 Lithuanian Property Records Stolen

Evidence: Confirmed by the victim or a government. Attribution: Unknown (prosecutors suspect a foreign state; President Nausėda spoke of "hostile states"). Conflict: Unproven.

Lithuanian prosecutors began investigating the theft of more than 600,000 records from the Real Estate Register run by the Centre of Registers, including personal identification codes. The intrusion happened earlier in 2026 and was found in April after a citizen complained about unusual interest in their property. The State Security Department confirmed that intelligence officers were among those affected.

Technical detail. The attackers logged in from abroad with the accounts of two Migration Department employees that had legitimate access to the register. The interior minister said there was no evidence those employees acted maliciously. No state has been formally named.

Sources: LRT, 29 May | LRT, 25 May | LRT on the president's remarks

June 13 and 23: Card and Banking Outages at Iranian State Banks (Rank 15)

Evidence: Confirmed by the victim or a government. Attribution: Unknown; the anti-government group Black Wolves claimed it. Conflict: Unproven; during the ceasefire.

On the evening of June 13, Iran's Coordination Council of Banks announced a "limited cyberattack" that took down mobile and internet banking, cash machines, card terminals, and card services at Bank Melli, Bank Saderat, Bank Tejarat, and the Export Development Bank. Card payments at petrol stations failed across the country. On June 23, card services at Melli, Saderat, and Tejarat went down again, and Iran's cyber command confirmed an attack on banking infrastructure. The banks said no customer data was accessed.

Technical detail. Experts quoted by AGBI say the attackers hit a shared communications platform used by the four banks rather than each bank's own systems, which would explain why they failed at the same time. Predatory Sparrow, which claimed earlier attacks on Iranian banks, was an early suspect but did not claim this one, unlike its usual habit.

Sources: IranWire | AGBI | Oman Observer

June 24 to 25: Ukraine's Postal App Knocked Out

Evidence: Confirmed by the victim or a government. Attribution: Claim (IT Army of Russia). Conflict: Russia–Ukraine.

Ukraine's state postal service, Ukrposhta, said its mobile app was temporarily out of action after an overnight "enemy" attack on its IT systems. The pro-Russian IT Army of Russia claimed it had broken in weeks earlier and stolen a user database; that claim is unverified.

Sources: The Record

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

June 25 to 26 (Disclosure): Turla's New Backdoor Against Ukraine

Evidence: Documented by credible technical research. Attribution: Researchers (Google: Turla). Conflict: Russia–Ukraine.

Google documented STOCKSTAY, a backdoor that Turla, a group widely tied to Russia's FSB, has developed since 2022. It was used mostly against Ukrainian government and military organizations, with some earlier activity against entities in Italy, the Netherlands, Poland, and Germany, including a foreign ministry.

Technical detail. It arrived through phishing sent from a hacked Ukrainian university mailbox and a diplomatic training website, through malicious remote desktop files and through installers named "DiplomacyEduAI." A November 2025 wave used an archive exploiting the WinRAR flaw CVE-2025-8088 against 20 targets in Ukraine.

Sources: SecurityWeek | The Hacker News

June 29: Israel Reports a Threefold Rise in Hostile Cyber Incidents

Evidence: Stated by officials or the media without technical detail. Attribution: Government statement (Israel National Cyber Directorate: Iran). Conflict: US/Israel-Iran.

Yossi Karadi, head of Israel's National Cyber Directorate, told Die Welt that Israel recorded 4,800 hostile cyber incidents in June 2026, against about 1,600 in June 2025. He said easier targets, such as law and accounting firms, often had their systems wiped, and that attacks on critical infrastructure had been repelled. These are reported incidents, not confirmed breaches, and no companies were named.

Sources: Al-Monitor (Reuters)

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

July to August 2026

The ceasefire with Iran collapsed on July 8, after attacks on ships in the Strait of Hormuz, and fighting resumed. (Wikipedia: 2026 Iran war · JINSA update, 21 October)

July 2 Onward: Russian Strikes on Kyiv's Internet Infrastructure (Context)

Evidence: Confirmed by the victim or a government. Attribution: Russia (physical strikes, claimed by its defense ministry in September). Conflict: Russia–Ukraine.

On July 2, a Russian attack damaged a key data center in Kyiv, disrupting several internet providers. On September 23, drones hit several data centers, providers, and a central traffic exchange; Ukraine's digital ministry said about 100,000 households in and around Kyiv lost or had poor internet. On September 27, Kyivstar, Ukraine's largest mobile operator, said its headquarters had been hit, and President Zelensky said a data center in Kyiv had been struck twice. Russia said the data centers served the Ukrainian military; Ukraine's foreign minister called them civilian infrastructure. These are physical attacks, not cyberattacks, but they show digital infrastructure becoming a direct military target.

Sources: Kyiv Independent | Reuters via The Star, 23 September | Reuters via The Star, 27 September

Early July (Confirmed August 13): AI Agents Used Against Taiwan's Government (Part of Rank 12)

Evidence: Confirmed by the victim or a government for the attack; documented by credible technical research (private firm) for the technical detail. Attribution: Unknown; Taiwan said it came from overseas. Conflict: China-Taiwan.

Taiwan's Ministry of Digital Affairs confirmed on August 13, after a Financial Times report, that government agencies were attacked in July by a campaign that combined ordinary hacking with AI agents such as OpenClaw. Alerts went out from July 20. The ministry said it had worked out the source, methods, and scope, that the affected agencies had cleaned up, and that the attacks "showed clear signs of originating overseas." It did not name a country.

Technical detail, from the Israeli firm Dream and not confirmed by the ministry. The framework ran on open-source agent software (Hermes and OpenClaw), with up to eight agents working at once, in 12 waves over about four days. It mapped 21 government systems, cracked 85 staff accounts, and took more than 2,500 personnel records, plus database passwords and single sign-on secrets. It used backup and test systems as stepping stones, and later scanned government IT suppliers, the nuclear safety regulator and at least seven energy companies. Its internal notes were in Simplified Chinese, which is used in mainland China, while the material aimed at targets used Traditional Chinese, which is used in Taiwan. That points toward a mainland operator but does not prove it.

Sources: Focus Taiwan | SecureWorld on Dream's findings | eSecurity Planet

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

July (Reported August 23): Small UK Generator Shut Down for Four Days

Evidence: Confirmed by the victim or a government. Attribution: Unknown; press reports blame hackers linked to Iran, but the UK government did not. Conflict: Unproven.

The Sunday Telegraph reported that a cyberattack shut down a small power generator in the UK for four days in July, and that Iran-linked hackers were blamed. The Department for Energy Security and Net Zero confirmed an incident at a small-scale generator and said "at no point was there a risk to the wider energy system." The site and the method were not disclosed.

Sources: The Irish Times | CNBC

July 13: EU and UK Sanction Russian Cyber Actors Together

Evidence: Confirmed by the victim or a government. Attribution: Government (EU and UK). Conflict: Russia-NATO hybrid pressure.

In their first joint cyber sanctions package, the EU listed nine people and four organizations and the UK 24 people and organizations. Those named include senior GRU officers, two members of the GRU's Unit 29155, members of the Cyber Army of Russia Reborn (CARR), the alleged leader of the Trickbot and Conti gangs, developers of the Lumma infostealer, and a bulletproof hosting service. The EU also named the FSB's 16th Centre, which controls groups including Turla, and referred to the failed December 2025 attack on Poland's energy sector.

Sources: BleepingComputer

July 23: Russian Group Steals Email Through a Zimbra Flaw

Evidence: Confirmed by the victim or a government. Attribution: Government (NSA, FBI and CISA with Dutch, British, Australian, Canadian, and other agencies: Laundry Bear, Russian state-sponsored). Conflict: Russia-NATO intelligence contest.

A joint advisory warned that Laundry Bear, also known as Void Blizzard, had used CVE-2025-66376 in the Zimbra email software as a zero-day from July 2025, and kept using it against servers that were not updated after Zimbra fixed it in November 2025. Targets include defense suppliers, government, energy, police, media, and NGOs, mainly in NATO countries and Ukraine.

Technical detail. The flaw is a cross-site scripting bug: code hidden in an HTML email runs as soon as the message is opened, with no click needed. It collects the last 90 days of email, passwords, the organization's address book and two-factor codes, and creates an app password (often named "ZimbraWeb") for later access. The data goes to rented servers that change every seven to 60 days.

Sources: Help Net Security | BleepingComputer

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

July 23: Intrusion at Saint-Noël Drinking Water Station, Quebec

Evidence: Confirmed by the victim or a government. Attribution: Unknown; the municipality said a Russia-based group was responsible. Conflict: Unproven.

At 07:30 on July 23, an intruder got into the drinking water station of Saint-Noël, a small town in Quebec. An employee spotted it quickly and the network was secured. The municipality said public health was never at risk and blamed a Russia-based group; federal authorities have not confirmed that.

Sources: Noovo Info

July 26 to August: The Wave Against US Water Utilities (Rank 4)

Evidence: Confirmed by the victim or a government. Attribution: Unknown; US officials quoted in the press call Iran the main suspect, but there is no official attribution. Conflict: Unproven, although it came during the renewed war and looks like the Iranian-affiliated campaign above.

On July 26 and 27, a coordinated attack hit the control systems of more than 30 Minnesota water and wastewater systems. Minnesota IT Services said the incidents shared timing, methods, and type of target. Braham's water plant went offline and residents were asked to save water; Plymouth lost links to two water towers and several pumping stations and ran them by hand; South St. Paul and Maple Plain lost automatic controls, and Maple Plain declared a local emergency. On July 30, the FBI and EPA warned that utilities in at least seven states had been hit since July 27, in some cases with lost water pressure and flooding. CISA later said more than 100 internet-facing water systems were targeted in July alone. No contaminated drinking water was reported anywhere.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Confirmed local cases:

Utility	Date	What happened	Source
More than 30 Minnesota systems	July 26 to 27	Braham plant offline; manual running in Plymouth; controls lost in South St. Paul and Maple Plain	The Hacker News
Coweta County, Georgia	July 27, around midnight	Attempt to change passwords and take over equipment; contact with controllers lost; attempt to move valves failed; manual running	WSB-TV
Clayton County, Georgia	Week of July 27	Pressure drops in north Clayton County; precautionary boil-water notice, later lifted; service back within hours	FOX 5 Atlanta
Cape May and Woodbine, New Jersey	July 27, from 01:30	Cape May: passwords changed, operators locked out of internet-connected parts; Woodbine: phone link to the system cut; water service never stopped	The Sun Papers
Rapid City, South Dakota	By July 31	Attempted intrusion at a wastewater pumping station, contained	KOTA-TV
Nine Michigan systems	Reported on Aug. 1 to 3	Activity matching the federal alert; all kept running safely	ClickOnDetroit
Columbus Water Works, Georgia	Confirmed on Aug. 15	Intrusion confirmed; drinking water not affected	Tenable
Two small private utilities, Colorado	Late Aug. (disclosed on Sept. 18)	Settings changed, alarms and remote access disabled, pump cycles altered briefly; each serves fewer than 200 people; water quality unaffected	Security Affairs

Technical detail. The FBI alert and Rockwell's advisory SD1790 of July 30 describe the method. The attackers reached Allen-Bradley MicroLogix 1100 and 1400 controllers (and some Micro820 and Micro850 models) that were directly reachable from the internet, often still on factory settings. They changed the controllers' network addresses and set passwords on devices that had none, which locked operators out and blinded them. At one utility they also rewrote the control program at several sites. No malware was needed.

Attribution. The method and the timing look like the Iranian-affiliated campaign in advisory AA26-097A, and US officials quoted in the press see Iran as the main suspect. But the FBI alert does not name anyone, Minnesota has made no attribution, and CBS and New Jersey officials reported that investigators were also checking whether another actor was posing as Iran. A Kansas supplier of water plant control equipment, Micro-Comm, was hit by the Barracuda ransomware gang in the same weeks; the FBI told the company that attack was random and unrelated.

Sources: Rockwell Automation SD1790 | Tenable | TechRadar on CISA's July figure | CBS News timeline | Reuters via WHBL on Micro-Comm

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

August 10 to 11: Ukrainian Intelligence Claims an Attack on Wildberries

Evidence: Stated by officials or the media without technical detail. Attribution: Self (Ukraine's HUR says its Cyber Corps did it). Conflict: Russia–Ukraine.

On August 15, Ukraine's military intelligence agency, HUR, said its Cyber Corps had disrupted Russia's largest online retailer, Wildberries, on August 10 and 11, taking down its main customer service channel, partly disrupting payments and overloading its call centers. HUR said the operation backed up drone strikes on Wildberries warehouses, which it accuses of serving Russian military logistics. Sellers did report payment delays, and Wildberries extended its payout period, citing "technical problems." The scale of the cyber effect has not been independently checked.

Sources: The Kyiv Independent | Ukrainska Pravda

From May (Disclosed August 11): Fake Job Interviews for Ukrainian IT Staff

Evidence: Documented by credible technical research. Attribution: Government (CERT-UA: UAC-0145, believed to be part of Sandworm). Conflict: Russia–Ukraine.

CERT-UA warned that since at least May, a group it tracks as UAC-0145 had posed as IT companies and recruiters, found system administrators through their CVs on job sites, moved the conversation to Telegram, and held English-language interviews on Zoom. The real targets are likely the telecom and IT firms where these people have privileged access.

Technical detail. As a "technical task," candidates had to connect to a company VPN using a modified WireGuard client called "SopraVPN," in one case through a domain imitating Sopra Steria. A hidden option in the client decrypts and runs PowerShell code; on Windows, it sets up a scheduled task and fetches more malware; and on Linux, it downloads a program through the VPN.

Sources: BleepingComputer | The Hacker News

August 19: US Advisory on Attacks Against Siemens Controllers

Evidence: Documented by credible technical research. Attribution: Unknown. Conflict: Unproven.

The NSA, CISA, and partners issued advisory AA26-231A on an active campaign against Siemens S7 controllers reachable from the internet, telling operators to find them, take them off the internet, tighten access, and check their control programs for changes. Public summaries name no victims, effects, or actor.

Sources: American Public Power Association

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

February to August (Disclosed August 20): Russian Phishing Aimed at Officials, Academics, and Defense Staff (Part of Rank 14)

Evidence: Documented by credible technical research. Attribution: Researchers (Google: two suspected Russian groups, UNC7005, and UNC5976). Conflict: Russia-NATO and Russia–Ukraine intelligence.

Google described two suspected Russian groups. UNC7005, which Google links to part of APT29, went after academics, diplomats, and NGO staff in Ukraine, Western Europe, and the US, and later the European defense industry. UNC5976, active since at least March, went after military, aerospace, and defense staff and think tanks, mainly in Ukraine and Armenia.

Technical detail. UNC7005 used fake invitations to diplomatic events to trick people into approving logins to their Microsoft accounts, pages that linked WhatsApp accounts to its own devices, common password-stealing malware, and in August, fake Google login pages using domains that imitated a Finnish defense industry body. UNC5976 used fake file-sharing pages with a "Continue with Google" button to collect access tokens, and a rogue Excel add-in. Google shut down their infrastructure.

Sources: Google Threat Intelligence | The Hacker News

Criminal Cases in the Same Period

Two incidents were linked to states in early reporting but turned out to be criminal.

- **Hungarian State Treasury, late July.** An intruder stole data from the Treasury's agricultural payments office and encrypted systems; the data was put up for sale. Early reports stressed traffic from Russian servers, but the attacker is a profit-driven individual known as ByteToBreach.

  Sources: Risky Business

- **Micro-Comm, Kansas, July 31.** The supplier of control equipment to wastewater plants found an intrusion; the Barracuda ransomware gang posted about 644 GB of files. The FBI told the company the attack was random.

  Sources: Reuters via WHBL

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

September to November 2026

September 8 (Disclosure): Sandworm Uses Google's Gemini Against Ukraine

Evidence: Documented by credible technical research. Attribution: Researchers (Google: Sandworm). Conflict: Russia–Ukraine.

Google's quarterly report on AI misuse said Sandworm had used the Gemini model in operations against Ukraine to gather information, prepare social engineering, and automate work, including writing scripts for password guessing and fingerprinting computers. This describes tradecraft, not a new attack with known effects.

Sources: Cyber Magazine

September 15: UK, US, and the Netherlands Expose Iranian Spyware

Evidence: Confirmed by the victim or a government. Attribution: Government (UK NCSC, FBI and Dutch AIVD: Iranian state actors). Conflict: Repression of Iranians abroad.

The three agencies published a joint advisory on CHOSEN BRICK, the Windows spyware used by Iranian state actors against dissidents, activists, and journalists worldwide, including in the UK. Personal details of some victims later appeared on pro-Iranian leak sites, which can put them in physical danger.

Technical detail. The operators posed as trusted contacts on WhatsApp and Telegram, built a relationship, and then got the target to download a file made for them, such as fake MRI results. Once installed, CHOSEN BRICK survives restarts, collects contacts, email, and social media messages, records the screen and the microphone, and can help track where the person goes.

Sources: NCSC | The National

September 2025 to July 2026 (Disclosed early October): Chinese Backdoor in Asian Governments

Evidence: Documented by credible technical research. Attribution: Researchers (Cisco Talos: China-nexus, high confidence). Conflict: China's regional rivalries.

Cisco Talos reported a group it calls UAT-11587 that had compromised at least 16 government and policy organizations in eight Asian countries by July 2026, about 350 computers in all, including defense ministries, parliaments, foreign ministries, border agencies, and think tanks. The biggest wave hit about 57 computers in India in two days in June.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. The backdoor, Antino, uses Microsoft's own cloud instead of a normal command server. Every 10 seconds, it checks an attacker-controlled Outlook mailbox for commands hidden in email subject lines, sends stolen files to one OneDrive folder, and fetches tools from another, so its traffic looks like ordinary Microsoft 365 use. Talos bases its assessment on Simplified Chinese language settings and a China time zone in decoy documents, among other clues.

Sources: Security Affairs | The Hacker News

October 1: Microsoft's Annual Threat Report Puts Israel Second Among Targets

Evidence: Documented by credible technical research (a company's measurement, not a list of incidents). Attribution: Researchers (Microsoft). Conflict: Several.

Microsoft's Digital Defense Report, covering July 2025 to June 2026, ranked the United States as the most targeted country (25.5 percent of the hostile activity it measured), followed by Israel (7.6 percent), Ukraine (4.8 percent), and Taiwan (3.9 percent). It said 39 percent of Iranian activity was aimed at Israel, 23 percent at the US, and 9 percent at the UAE.

Sources: Ynet

October 8 (Disclosure): Russian-aligned Malware in Ukrainian Industry

Evidence: Documented by credible technical research. Attribution: Researchers (ESET: UAC-0099, aligned with Russia, medium confidence). Conflict: Russia–Ukraine.

ESET reported that UAC-0099 infected a Ukrainian manufacturer in December 2025 and an energy company in June 2026 with a downloader called MATCHBOIL. ESET thinks the group may break into victims and then hand them to Sandworm. On October 23, further reporting described exactly that: UAC-0099 got into a Ukrainian logistics company in July 2025 and passed access to Sandworm, which wiped data on September 17, 2025, using Microsoft's own SDelete tool. That wiper attack predates this period and is mentioned only to show the hand-off model.

Technical detail. A phishing link downloads an archive with a script that fetches MATCHBOIL, which installs its payload, makes itself persistent and checks in every two minutes with servers hidden behind Cloudflare.

Sources: ESET | SC Media

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

October 8: FBI Seizes Tools of a Chinese Government Contractor

Evidence: Confirmed by the victim or a government. Attribution: Government (US with the UK, Australia, Canada, Japan, New Zealand, and Spain: Integrity Technology Group, Flax Typhoon). Conflict: China strategic operations.

The Justice Department and FBI seized seven domains used by Integrity Technology Group, a Beijing contractor for the Chinese government linked to Flax Typhoon. A seven-country advisory named the company for building and selling hacking tools and for breaking into networks. Court papers say it also ran a botnet of hijacked internet devices that held more than 1.2 million infected devices in its database as of June 2024. Targets included a power company in South Carolina, airports in Japan and Poland, gas and power companies, and universities in Taiwan.

Sources: US DOJ | The Hacker News

From October 6: DoS Attack on a St. Petersburg Internet Provider

Evidence: Confirmed by the victim or a government for the outage; claim by the actor only for the break-in. Attribution: Claim (The Ukrainian group BO Team). Conflict: Russia–Ukraine.

SkyNet, a large internet provider in St. Petersburg, said a DoS attack had disrupted its network since October 6, affecting gaming, calls, and video conferencing. BO Team, also known as Black Owl, claimed attacks on September 14 and October 5, said it had disabled more than 15,000 network devices, and posted screenshots it says came from SkyNet's internal systems. SkyNet only confirmed the DoS attack.

Sources: The Record

October 9 to 14: Ukrainian Drones Hit Russian Data Centers (Context)

Evidence: Confirmed by the victim or a government. Attribution: Ukraine (physical strikes, presented by President Zelensky as retaliation). Conflict: Russia–Ukraine.

On October 9, Yandex reported drone strikes on two of its data centers, in Sasovo and in the Kaluga region; a third, near Vladimir, went fully offline over the weekend of October 10 and 11. Yandex apps and payment services and businesses using Yandex's cloud were disrupted, including for users in Central Asia and Armenia. On October 14, drones hit a Sberbank data center under construction in Balakovo. Zelensky said the strikes answered Russia's attacks on Kyiv data centers. Like the Russian strikes, these are physical attacks, but they show both sides now treat data centers as military targets.

Sources: The Moscow Times, October 12 | The Moscow Times, October 14

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

October 13: Attack on More than 100 Azerbaijani Government Websites

Evidence: Confirmed by the victim or a government. Attribution: Unknown officially; claimed by 313 Team, which is reported to be linked to Iran and based in Iraq. Conflict: Iran-Azerbaijan tension, unproven.

From 22:00 local time on October 13, Azerbaijan's State Service for Special Communication and Information Security reported an attack by "a foreign hacker group" on more than 100 government domains. Access to several government websites was disrupted, but the sites kept running. 313 Team claimed it, citing a supposed headscarf ban in schools; its claims of 1,825 sites taken down and 2.5 Tbps of traffic are unverified and far above the official figure.

Sources: Azernews | Bernama

Late August to October 15: BeyondTrust Zero-day Used by a Chinese Group (Part of Rank 13)

Evidence: Confirmed by the victim or a government. Attribution: Researchers (Google Mandiant: Armory Castle, formerly UNC5221, suspected China-nexus). Conflict: Strategic espionage.

BeyondTrust disclosed on October 15 that its Remote Support product, up to version 26.2.3, had been attacked since late August through a previously unknown flaw, CVE-2026-102764. It patched its cloud customers by October 9; customers running it themselves must install patch BT26-05-RS. Victims were not named. Google expects Armory Castle to exploit the flaw widely now that it is public, as it did with Ivanti flaws in 2024.

Technical detail. The flaw lets an attacker upload files to the appliance without logging in. The attackers installed a hidden web shell and a tunneling tool, gave themselves permanent administrator rights, read the appliance's store of secrets, used a compromised administrator account to watch remote support sessions and copy files, and deleted logs. A remote access appliance trusted by thousands of organizations can become a door into all of them.

Sources: Google Threat Intelligence | BeyondTrust BT26-05 | BleepingComputer

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

October 21 to 22: Taiwan Reports More Chinese Cyber Pressure Before Local Elections

Evidence: Documented by credible technical research. Attribution: Government (Taiwan National Security Bureau: China). Conflict: China-Taiwan.

Taiwan's National Security Bureau told lawmakers that the government network averaged about 2.6 million intrusion attempts a day in the first nine months of 2026, rising sharply since June, and that more than 2.5 million pieces of disinformation were attributed to China, up from about 1.7 million a year earlier. The bureau suspects the rise is linked to preparations to interfere in the November 28 local elections, including hacking specific people to steal election-related information. These are attempts and detections, not confirmed breaches.

Sources: Focus Taiwan | The Manila Times

October 19 to 23 (Disclosed in late October): Breach of Moldovan Government Services

Evidence: Confirmed by the victim or a government. Attribution: Government suspicion of a foreign state actor, no country named. Conflict: Unproven; Moldova has repeatedly accused Russia of hybrid campaigns.

Moldova's Electronic Governance Agency said attackers extracted data from government services between October 19 and 23, when access was blocked; two more attempts after that failed. They made about 11 million requests and reportedly extracted data associated with approximately 750,000 personal identification numbers (IDNPs), a preliminary count that should not be treated as a confirmed number of distinct affected individuals. The data may include names, birth details, family links, health insurance and benefits status, disability records, driving licenses, and photos, vehicles and companies owned, bank account numbers (IBANs), tax debts, and payment histories. Bank card data was not affected and no state records were altered. As a precaution, 82 digital services were checked and the vulnerable ones taken offline, along with more than 30 information systems. President Sandu's office called a National Security Council meeting on October 29.

Prime Minister Vasile Tofan called the attacks "coordinated and large-scale" and told Euronews, "We suspect the state actor to be behind it," adding, "I don't think the list of suspects is very long." The head of the national cybersecurity agency, Mihai Lupaşcu, called it the largest cyberattack Moldova has recorded, said AI tools were probably used and said it was premature to name an actor.

Technical detail. The attackers abused government services that could be reached without logging in, then used what they found to pull more data from connected systems.

Sources: The Record | RFE/RL | Euronews | Newswav copy of the Euronews interview | Moldova Electronic Governance Agency

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

October 22 (Disclosure): Iran's Prince of Persia Group Spies on Dissidents from US Servers

Evidence: Documented by credible technical research. Attribution: Researchers (Semperis: Prince of Persia, an Iranian state-sponsored group). Conflict: US/Israel-Iran.

On October 22, the security firm Semperis said its researcher Tomer Bar had found a command server of Prince of Persia, an Iranian state-sponsored espionage group active for about two decades, at a US hosting company. Semperis found the server in August 2026 and says it is only the second time it has seen the group host in the US, the first being in 2016; the group normally uses European hosting. Recent victims are mainly Iranian dissidents, and the group has also targeted public and private organizations in the US, Europe and the Middle East. According to Semperis, the group went quiet when the war began on February 28, then came back on shared hosting, behind Cloudflare and with a new management panel.

Technical detail. The group's tools are known as Foudre (a first-stage loader), Tonnerre (full surveillance, including documents, hidden screenshots, and audio recording) and a newer tool, Tornado, which can use HTTPS and the Telegram API as a hidden command channel. Semperis also describes domain-generation algorithms and exfiltration through blockchain services. Reports differ on how long it had been since the group last used US servers: Semperis's own release says about ten years, while Infosecurity Magazine wrote "at least 12 years"; this report follows Semperis.

Sources: Semperis press release | Infosecurity Magazine | Iran International | Semperis original research

October 23 to 24: Palo Alto Firewalls Rooted with a Custom Exploit

Evidence: Documented by credible technical research. Attribution: Researchers (Dream; tooling and results independently checked by Palo Alto Networks Unit 42). Possible China-linked operator, not established. Conflict: Suspected Indo-Pacific espionage; state direction unproven.

Dream researchers reported finding evidence of an operation that compromised 25 PAN-OS firewall and management servers across the United States, Japan, Taiwan, and South Korea. Artifacts recovered on October 25 indicated that the intrusions had already taken place. Three servers in a US government-affiliated environment received particular attention, and researchers found evidence of access to internal Active Directory information and credentials. The original incident dates and the complete outcome of subsequent actions remain uncertain. Palo Alto Networks subsequently verified the attacker tooling and results.

Technical detail. The attackers wrote their own exploit for two flaws in PHP, CVE-2026-109618, and CVE-2026-109619 (nicknamed PHP2Shell), tailored to PAN-OS 12.1 and 12.2, which run PHP 8.0.30 with a large memory limit. They chained it with Fragnesia, CVE-2026-46300, a Linux kernel flaw, to get root. The chain took under fifteen minutes and was followed by about 40 custom scripts. Dream identified an AI-oriented offensive platform, Chinese-language model integrations, Claude Code, and FOFA access keys in the recovered environment. These indicators suggest possible China-linked activity but do not prove the operator's nationality or state

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

sponsorship. Dream explicitly said it had no direct evidence that AI wrote the exploits or post-exploitation scripts. Whether password spraying, backdoor accounts, and theft of SAML signing keys succeeded is not known. In a later update, Palo Alto Networks said about 0.02 percent of its installed base had affected internet-facing management interfaces.

Sources: The Register | Help Net Security | Infosecurity Magazine | Dream Research | Palo Alto Networks Unit 42 confirmation

October 24 to 27: Iranian Pressure Around Israel's General Election

Evidence: Documented by credible technical research. Attribution: Handala, which the US DOJ says is a front for Iran's Ministry of Intelligence. Conflict: US/Israel-Iran.

On October 24, Haaretz reported that Handala had published personal and military-related information about a senior IDF officer. The IDF said the alleged breach was under investigation, and the means of access were not disclosed. On October 25, Check Point reported an average of approximately 2,700 attempted cyberattacks per monitored Israeli organization per week during early October, up 55 percent year over year. CTech reported about 2,300 weekly attempts against government organizations, up 82 percent, and about 3,900 against energy and infrastructure, up 107 percent; a separate media summary gave a different government sector figure, so these sector numbers should be treated as reported vendor telemetry rather than independently reconciled totals. Separately, Check Point said it had verified roughly 87 incidents since October 1, mainly website takedowns and defacements. It also identified more than 1,200 election-related website registrations, including suspected phishing pages, and noted the reappearance of a previously leaked voter database. These measures are not a count of successful intrusions across Israel.

On election day, October 27, Handala posted photos and videos of flower bouquets with letters that it said it had left at polling sites and at a place linked to the candidate Gadi Eisenkot. The National reported no sign that the bouquets posed any threat. This was a physical stunt, not a cyberattack, but it shows how the persona mixes hacking, leaks and intimidation.

On October 29, the Telegraph, quoting anonymous Iranian officials, reported that Tehran had set up groups to hack election systems in Israel and the US. The report itself did not show that any voting system was breached. It is listed below as unproven.

Sources: Haaretz (paywalled original) | Jewish Rhody, summarizing Haaretz | CTech on Check Point's findings | The National | The Jerusalem Post on the Telegraph report | CTech report summarizing Check Point findings

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

October 28 (Disclosure): First Belarus-aligned Destructive Attack in Ukraine

Evidence: Documented by credible technical research. Attribution: Researchers (ESET). Conflict: Russia–Ukraine; Belarus-aligned activity overlapping Russian wartime objectives, without proof of direct Belarusian state direction.

ESET's APT Activity Report for April to September 2026 contains several findings relevant to the war. The most important is that FrostyNeighbor, a group aligned with Belarus and also known as Ghostwriter, carried out a destructive attack on a Ukrainian manufacturer that plays an important role in the transport sector. ESET says it is the first destructive attack by a Belarus-aligned actor it has documented in Europe, and it sees Belarusian groups increasingly acting as force multipliers for Russia. The victim and date were not given.

Other points from the report: a large Russia-aligned campaign exploited MDaemon mail servers in Ukraine and installed two backdoors, HELLAGE and HELLTAG; a group called PhantomCaptcha tried to plant Android spyware, PrincessSpy, while posing as Ukrainian organizations; Gamaredon's activity fell sharply, possibly because of Ukrainian strikes on Crimea, where the group is believed to work; and North Korean groups now target Ukraine more often, which ESET links to North Korea's part in Russia's war. One group, UAC-0099, hid a fake request for nuclear weapon instructions in a script comment, apparently to make AI-based analysis tools refuse to look at the code.

Sources: ESET APT Activity Report Q2 to Q3 2026

October 28 (Disclosure): Volt Typhoon's Silent Train Relay Network

Evidence: Documented by credible technical research. Attribution: Researchers (Lumen Black Lotus Labs: Volt Typhoon, Chinese state-sponsored). Conflict: China-US, possible preparation for a crisis in the Pacific.

Lumen's Black Lotus Labs said it has followed for three years a relay framework it calls Silent Train, which Volt Typhoon uses to hide where its attacks come from. Through it the group exploited at least four zero-days in network edge and management products: VeloCloud Orchestrator (CVE-2026-16812), Cisco Catalyst SD-WAN (CVE-2026-20127), N-able N-central (CVE-2025-8875 and CVE-2025-8876) and, earlier, Versa Director (CVE-2024-39717), with a suspected zero-day in Quest KACE. Targets included telecoms, government, defense contractors, utilities, satellite providers, managed service providers, transport, aviation, and emergency services. California, Texas, and Hawaii were the most targeted states, which Lumen assesses as consistent with strategically motivated interest in the Indo-Pacific; observed geography alone does not establish a specific wartime objective. US agencies have previously warned that Volt Typhoon pre-positions inside critical infrastructure so it could disrupt it in a conflict.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. Traffic goes from servers outside the US through hijacked home and small-office devices, such as Intelbras modems abroad and Netgear Orbi routers in the US, chained over SSH. Only the minimum is installed on each relay, and everything is removed after each session, which usually lasts under eight hours. Lumen says the network grew after the FBI took down Volt Typhoon's earlier KV-Botnet. The attribution partly rests on inference, such as working hours on China Standard Time.

Sources: BleepingComputer | Nextgov | Lumen Black Lotus Labs

October 28 to 29 (Disclosure): VMware Logging Flaw Used as a Zero-day

Evidence: Documented by credible technical research. Attribution: Researchers (CrowdStrike: WARP PANDA, China-nexus). Conflict: Strategic espionage.

CISA added CVE-2026-41709, a low-rated flaw in VMware ESX, to its list of exploited vulnerabilities on October 28. CrowdStrike says WARP PANDA, the group Google calls Armory Castle (formerly UNC5221) and the one behind the BeyondTrust zero-day in the main review, used it as a zero-day in early 2026, mainly against US law firms. The flaw can suppress logs for certain operations performed with administrative access; it does not by itself provide initial entry into a system. CrowdStrike assessed that it helped the operators conceal activity inside virtual environments.

Technical detail. The group gets in through edge devices, moves to VMware vCenter, installs BRICKSTORM and SharpStorm, steals session tokens to reach Microsoft 365 without triggering password alerts, and in one case registered its own MFA device on a victim account. Broadcom fixed the flaw in July 2026.

Sources: The Hacker News | Help Net Security | CrowdStrike original analysis

October 29: About $6.3 Billion Stolen from Binance

Evidence: Confirmed by the victim or a government. Attribution: Government (FBI: TraderTraitor, North Korea). Conflict: North Korean state revenue under sanctions.

On October 29, attackers stole approximately $6.34 billion in digital assets through unauthorized use of Binance's internal wallet-signing service, according to Binance's November 3 investigation update. Elliptic, which puts the loss at $6.43 billion, counts eleven blockchains, with Ethereum the largest share at about $3.8 billion, followed by Tron, Bitcoin, the XRP Ledger, Solana, and others. Binance stopped withdrawals. On October 31, the FBI said North Korea's TraderTraitor group, which it also blamed for the $1.5 billion Bybit theft in 2025, was behind it, and asked exchanges to block transactions linked to the wallets it named. The same day, President Trump said investigators did not yet know whether North Korea was involved, so the FBI finding should be read as the official US assessment rather than a closed case.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Binance reported approximately $2.85 billion frozen or intercepted as of November 3, subject to reconciliation and market movements. These assets were not necessarily returned to Binance. Separately, Binance said it had replenished 98 percent of affected token assets by October 31, using its own financial resources; this was not equivalent to recovery of the stolen funds. TRM Labs and Elliptic both attributed the theft to TraderTraitor with high confidence before the FBI did. Accounts of the timing differ: TRM said most of the funds left in about twenty minutes, while Elliptic describes draining that began around 20:05 UTC and went on for about three hours across all chains. Elliptic also found some of the stolen funds being laundered together with proceeds of the September 2026 theft from the Bitget exchange, which it assesses as highly likely North Korean.

Binance said it would cover the loss itself, from its SAFU user fund, a Bitcoin reserve, an insurance fund and corporate treasury, and withdrawals restarted around November 1. On November 3, North Korea's state news agency KCNA quoted Kim Yo Jong calling the US claim "an absurd rhetoric" and "a grave political provocation."

Technical detail, as published so far. Binance says the operation began with a fake job offer. Someone posing as a project director contacted one of its engineers through a job platform, two rounds of fake interviews followed, and the engineer downloaded an "assignment" that gave the attackers a foothold. Separately, another engineer installed a tampered Homebrew package from an advert; Binance removed it, but the attackers learned who managed the wallets. From the first laptop, and with the help of an internal AI tool, they took over the accounts of a wallet DevOps engineer and a wallet software engineer. The DevOps engineer's machine held a container deployment token that let them get Binance's own signing system to approve withdrawals, so the blockchains accepted the transfers as genuine. On Ethereum, CoinDesk's analysis shows how about $2.5 billion left one wallet, labeled Binance 14, in under four minutes. Using EIP-7702, a feature added to Ethereum in 2025 that lets an ordinary wallet run a smart contract's code, the attacker had the wallet sign an authorization pointing to a "sweeper" contract only the attacker could operate. At 20:24 UTC, the sweeper moved about 167,464 ETH and 63 tokens, including roughly 1.6 billion USDT; the wallet revoked the permission at 00:10 UTC the next day, after nearly four hours. How the attacker obtained the signatures is not yet public. Binance says the attackers used tools that deleted their traces, and that it found no sign that any wallet private key leaked; after first pointing to a single compromised laptop, it later reported additional points of breach. Its full report is still pending, so some of these details may change.

Note on figures. Binance says about $6.3 billion, TRM about $6.36 billion and Elliptic $6.43 billion. Binance's share of losses already replaced was given as 90 percent and later 98 percent.

Sources: Al Jazeera on the FBI attribution | Fortune on Binance's account | ITV News | Elliptic analysis | CoinDesk on the EIP-7702 drain | Hawaii News Now (CNN) on TRM and Chainalysis | Devdiscourse (Reuters) on North Korea's denial | Binance initial investigation | FBI TraderTraitor attribution

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

October 29 (Disclosure): Suspected Hack of Freezers at US Military Commissaries

Evidence: Stated by officials or the media without technical detail. Attribution: Unknown; US officials quoted anonymously suspect Iran-linked hackers. Conflict: Unproven, although it happened during the US-Iran war.

Reuters, citing four officials, and Nextgov reported that the Pentagon is treating freezer failures at at least six US military commissaries, the on-base grocery stores, as a suspected cyberattack. The failures began in late August. At Fort Huachuca in Arizona, the base said on August 26, that a freezer "went into defrost mode where it heated up all the food." US Cyber Command and the Army Criminal Investigation Division's Cyber Field Office are involved and are working with French authorities, who are investigating similar attacks on French supermarkets in October. Two people familiar with the matter told Nextgov that officials suspect Iran-linked hackers, but Nextgov stressed the assessment could change. No official has said so on the record, and how the attackers got in has not been disclosed.

Sources: Nextgov, October 29 | Nextgov on the Iran suspicion | ThePrint (Reuters exclusive)

October 31 to November 1: Claimed Destructive Attack on Rosstat

Evidence: Stated by officials or the media without technical detail. Attribution: Claim (Belarusian Cyber Partisans and the pro-Ukrainian group Silent Crow). Conflict: Russia–Ukraine, with Belarusian opposition involvement.

On November 1, the Belarusian Cyber Partisans and Silent Crow said they had attacked Rosstat, Russia's federal statistics service, overnight on October 31. Kommersant reported that the main Rosstat website and regional portals were defaced with a warning in Belarusian, "No one will escape accountability," and the groups say they put up Ukrainian figures on Russian military losses for about an hour. Rosstat confirmed it had been targeted but said its systems spotted suspicious activity in time, and that it had found no evidence of leaked protected data or compromised databases.

What the groups claim. About six months inside the network, four of them spent quietly collecting documents; access to about 25,000 computers and devices at headquarters, regional offices and a data center; theft of census, mortality and economic data, internal correspondence, statistics on occupied Ukrainian territories, and data on Russian military casualties; and a final phase that wiped physical and virtual servers and storage. They say they controlled domain controllers, virtualization platforms, and management tools. None of this has been independently confirmed, and Rosstat disputes the theft and destruction.

Sources: The Record | Kommersant reporting of Rosstat statement

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

November 1: False Nuclear and Chemical Alerts Through Ukraine's Air Alert App

Evidence: Stated by officials or the media without technical detail. Attribution: Government accusation (Ukraine blames Russia); claim by a group calling itself Hitcore. Conflict: Russia–Ukraine, psychological operation.

At about 22:48 Kyiv time on November 1, the evening the Kherson truce ended, users of Povitriana Tryvoha (Air Alert), the official and widely used app for warnings of air attacks, began receiving false messages. They warned of a nuclear threat across Ukraine, high radiation, a chemical threat and street fighting in Kyiv, and one message, in Russian, referred to the Oreshnik missile. The Kyiv map in the app showed several danger markers at once, while a real alert for jet drones was also active in the region. At 23:02, Ukraine's Air Force said the app had "probably been subjected to hostile influence" and that there was no radiation threat. Ukraine's Centre for Strategic Communications blamed Russia. A Russian Telegram channel said a group called Hitcore had done it; that claim has not been verified and nothing is known about the group.

Technical detail. The app was built by the security company Ajax Systems with the developer Stfalcon. The developers switched off push notifications and took the app offline, and Ajax said the main functions, the alerts, and the danger map, were back within about two hours. Ajax said no data leaked and that the app does not store users' personal data. How the attackers got the ability to send notifications has not been published. The messages mixed English, Russian, and Ukrainian and contained spelling mistakes. The Air Force stressed that the app is separate from military command systems, and sirens and official channels kept working.

Why it matters. Sending a fake nuclear alarm through the country's main warning app is a psychological attack aimed straight at civilians. It also tests how far people will keep trusting the app when real attacks come.

Sources: Al Jazeera | PBS NewsHour (AP) | dev.ua (Ukrainian) | DOU (Ukrainian)

November 1 to 3: Attacks on Supermarket Refrigeration Controllers Across Europe

Evidence: Stated by officials or the media without technical detail. Attribution: Unknown; no claim. Conflict: Unproven.

Overnight on November 1 to 2, attackers changed the settings of refrigeration controllers in shops across Europe, putting units into defrost mode or setting them as high as 50°C (122°F), so that food had to be thrown away. Reported cases, in at least nine countries, include several dozen Delhaize stores in Belgium and Luxembourg, 15 Carrefour stores and 10 to 15 Intermarché stores in Belgium, five Spar shops, an IKEA store in Mons, 13 SuperValu stores in Ireland, six or seven Coop stores in Sweden, stores in Portugal, Italy, Finland, and Estonia, and at least 17 small businesses, mostly butchers, in the Netherlands. Belgium's federal prosecutor opened a criminal investigation. The European Commission said it was coordinating with member states through CyCLONe, the EU network for large-scale cyber crises, and Agriculture Commissioner Christophe Hansen called the attacks a "deliberate attempt to disrupt" the EU food supply, while saying food security was not at risk.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Technical detail. The devices named in France's CERT-FR alert are Danfoss AK-SM and AK-SC controllers and Copeland and Dixell XWEB units reachable from the internet. Danfoss reported that some Dutch installations had retained default passwords and insufficiently protected internet access despite its October 13 advice; this finding cannot be extended to every European victim. Many older units, such as the AK-SM 800 and AK-SC 355, no longer get updates. Claroty had previously published vulnerabilities affecting related products, but the available evidence does not establish that these particular flaws were used in all incidents. Public reports chiefly describe unauthorized changes to refrigeration settings; malware use has not been established.

Attribution. No one has claimed the attacks and no government has named a suspect. Belgium's Centre for Cybersecurity said it is unknown who is responsible and that this "may never be determined." SentinelOne researcher Tom Hegel told Reuters that the absence of ransom demands points to sabotage rather than extortion, but that from the defender's side, a teenager and an intelligence service "would look much the same." European officials have warned more broadly of Russian sabotage in Europe, but nothing published ties these attacks to Russia, Iran or anyone else, and a shared method does not prove a shared attacker.

Sources: The Star (Reuters) | The Hacker News | Smartworld on CyCLONe (Italian) | NL Times | Al Jazeera

November 2 (Disclosed November 3 to 4): Supplier-linked Attack Affects French Blood Service Refrigeration

Evidence: Stated by officials or the media without technical detail. Attribution: Unknown; supplier involvement confirmed, intrusion path still under investigation. Conflict: Unproven; no evidence of state direction or connection to supermarket attacks.

France's national blood service, Établissement Français du Sang (EFS), confirmed that temperature and defrost settings had been altered at three refrigeration sites on November 2. The affected equipment was remotely managed by an external refrigeration provider. Monitoring alarms alerted staff, who secured or transferred the stored products. EFS reported no loss of blood products or samples, no health impact and no interruption of blood collection or distribution. The incident demonstrates the risk of third-party access to systems supporting sensitive healthcare logistics; it does not establish compromise of EFS's wider IT environment.

Technical detail. Coolworld separately acknowledged an incident involving refrigeration remote-monitoring software and said the reported vulnerability involved a third-party component. The company did not name EFS as a customer in its statement. EFS did not publicly identify its supplier, and a direct connection between this incident and the retail refrigeration attacks had not been established as of November 5.

Sources: Reuters, November 4 | Associated Press, November 4 | Coolworld company statement

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

November 2: False Alerts Through Russia's Emergency Warnings App

Evidence: Stated by officials or the media without technical detail. Attribution: Unknown officially; President Zelensky said Ukraine responded to the Russian attack, without describing what was done. Conflict: Russia–Ukraine.

At about 02:45 Moscow time on November 2, a few hours after the Ukrainian incident, Russia's Emergencies Ministry (MChS) said its mobile warnings app, which alerts users to incoming drones, had suffered a "massive cyberattack" and had sent false information. According to AP, the false alert reached users in 33 of what Russia counts as its 89 regions. The ministry said it had found the weakness and was taking "necessary measures," and that SMS warnings, broadcasts, and sirens were working normally. It did not say who was responsible.

In a November 2 PBS NewsHour interview, President Zelensky was asked directly whether Russia had attacked Ukraine's warning system and Ukraine had hacked Russia's system in response. He agreed and, when specifically asked whether Ukraine had hacked the Russian emergency application, replied, "Yes, absolutely. We just responded on the attack." This constitutes public acknowledgment by Ukraine's president of a retaliatory cyber operation. It does not independently establish the detailed intrusion method, its full scope, or which operators implemented it.

Technical detail. None has been published.

Sources: PBS NewsHour (AP) | PBS NewsHour, Zelensky's remarks | Al Jazeera | PBS original interview transcript

November 4: Kyiv Independent Website and Newsletter Hijacked

Evidence: Stated by officials or the media without technical detail. Attribution: Suspected Russian, by the victim, based on the content of the messages. Conflict: Russia–Ukraine, psychological operation.

The English-language Ukrainian newspaper the Kyiv Independent said attackers had got into its website management system and its newsletter service. They posted false messages on the site, which staff removed quickly, and emailed subscribers in Russian and English. One email falsely said President Zelensky had launched a nuclear warhead at Kyiv as "proof of friendship" after meeting Putin and told readers to take shelter, giving a Telegram channel name. Others made up a physical attack on Zelensky. The paper said readers' and donors' bank details were not exposed because payments go through outside services.

Technical detail. Only the two entry points, the content management system and the mailing service, have been disclosed. The paper gave no technical evidence for the Russian link, and there is no confirmed connection to the Air Alert incident, although both pushed a fake nuclear alarm within days of each other.

Sources: The Record | The Kyiv Independent

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

November 4 to 5 (Disclosure): Midnight Blizzard Plants Phone Exploits on Ukrainian and European Websites

Evidence: Documented by credible technical research. Attribution: Researchers (Sekoia: APT29/ Midnight Blizzard assessed with moderate-to-high confidence; widely linked to Russia's SVR). Conflict: Russia–Ukraine and Russia-NATO intelligence.

Sekoia, which found the activity in mid-October and calls it "Poisoned Source," reported a watering-hole campaign against iPhone and Android users in Europe and the US, through compromised websites and impersonation infrastructure observed in the US, Ukraine, the Czech Republic, and Bulgaria; the full number of compromised users is not public. Code was injected into the website of a Ukrainian gas production company, an industry trade association (a US chemical industry body, according to The Hacker News), a European far-right party and a Bulgarian military-related site. Most notably, the attackers compromised Plerdy, a Ukrainian web analytics provider, so that its tracking script carried the malicious code to hundreds of sites, including army, special forces and military equipment sites, from August 27 to September 3, 2026. Two look-alike domains imitated america250.org and the Raffles London hotel, which Sekoia thinks were aimed at diplomatic delegations and high-profile guests; other look-alikes targeted Ukraine, the Czech Republic and Bulgaria. Sekoia explicitly assesses the APT29 connection with moderate-to-high confidence, based on technical overlaps, operational patterns, victimology, and infrastructure.

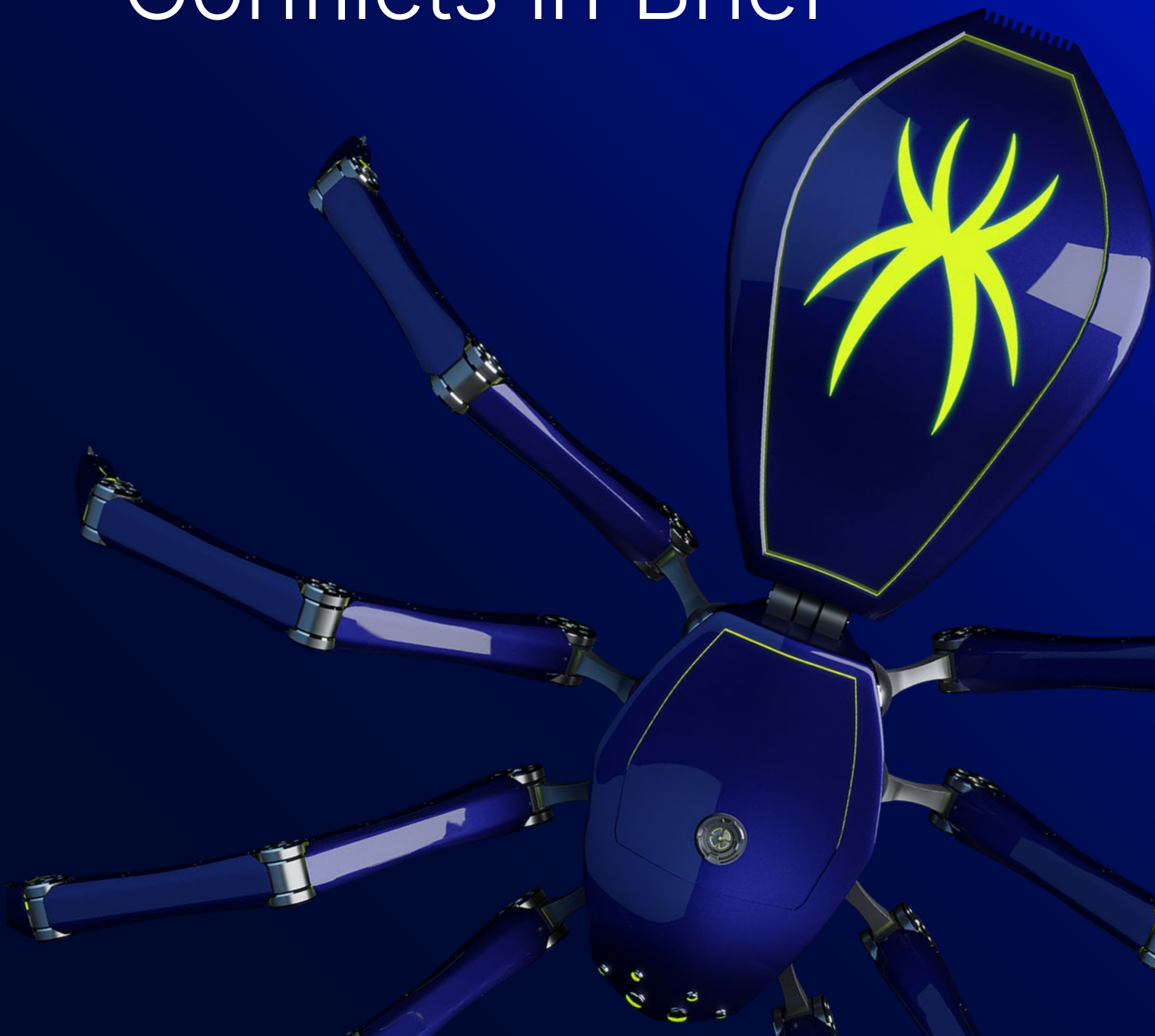
Technical detail. Visitors were first fingerprinted. Suitable iPhones got one of two chains built on DarkSword, the exploit kit that leaked earlier in 2026, one of them combined with CVE-2024-27834. Android phones got a chain using CVE-2026-3910 in Chrome and CVE-2025-27038 in Qualcomm drivers. The observed exploit chains relied on previously patched vulnerabilities; their presence does not establish that every visitor was successfully compromised. The iPhone payload collects messages, email, voicemail, passwords, contacts, calls, calendars, photos, and iCloud Drive files; the Android payload, AndroSnitch, steals Chrome cookies, passwords, and Wi-Fi passwords. Sekoia notes that recycled commercial exploit chains make advanced phone hacking cheaper for state groups.

Sources: SecurityWeek | The Hacker News | Sekoia original technical report

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Appendix C: The Main Conflicts in Brief



LevelBlue SpiderLabs

Russia and Ukraine

Russian operations against Ukraine were mostly about intelligence: phishing with new Office and Zimbra flaws, iPhone exploits on Ukrainian websites, the Turla and MATCHBOIL backdoors, and account takeovers. The destructive side, led by Sandworm, used new wipers over the winter and, by ESET's account, once reached into a NATO country with the Polish energy attack. Ukrainian officials say intrusions into energy companies now serve missile targeting. Ukraine's own operations are visible mostly through its own claims, such as Wildberries, and through volunteer groups such as BO Team. From July, and especially in September and October, both sides struck each other's data centers with drones and missiles, which caused more disruption to everyday digital services than any confirmed cyberattack in the war this year.

The United States, Israel, and Iran

This was the busiest cyber theater of the period. The US openly described cyber effects at the start of its strikes. Iran answered mostly through fronts of its Ministry of Intelligence (Handala, Homeland Justice) and groups linked to its Revolutionary Guards: wipers at Stryker and the Albanian Parliament, tampering with US industrial controllers, an attempt on Jordan's grain silos, camera hijacking, leaks, and intimidation. On the Iranian side, the government's own blackout did more to cut people off than any foreign attack, while unclaimed operations hijacked Iranian apps, TV channels and bank card systems. The fighting resumed on July 8, and the US water wave came three weeks later, but no government has linked the two.

Israel and Hamas

Since the Gaza ceasefire of October 10, 2025, the cyber activity attributed to Hamas-linked groups has been mostly espionage against Arab governments and the Palestinian Authority (Ashen Lepus), plus a possible link to the fake rocket alert app in March. There was no confirmed destructive Hamas-linked attack on Israel found in this period. Most of the cyber pressure on Israel came from Iran: the Shamir hospital attack, the Clalit claim, leaks by Handala, camera hijacking, and mass text messages. Israel's cyber directorate reported a threefold rise in hostile incidents by June 2026.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

China, Taiwan, and the Wider Indo-Pacific

China-nexus groups were the most technically capable espionage actors: inside Singapore's telecom operators, in 42 countries through Google Sheets, in Asian governments through Outlook, and in remote access appliances through new zero-days. Norway and the UK both acknowledged Salt Typhoon activity. Taiwan reported millions of daily intrusion attempts and an AI-agent campaign it did not formally attribute. The US and six partners took action against a Chinese contractor that built and sold hacking tools.

North Korea

North Korea's operations were about money: Upbit in November 2025, Drift and KelpDAO in April 2026, and the Axios package hijack, with TRM Labs estimating about $643 million stolen in the first half of 2026. ESET also reported continued espionage against European drone makers.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Appendix D: Patterns: Actors, Actions, and Ways of Working



LevelBlue SpiderLabs

By Operator

Operator	Incidents in this Report	Typical Behavior	How Strong the Attribution Is
Russian military intelligence (GRU): APT28, Sandworm, and related groups	Office zero-day phishing, hijacked routers, Sandworm wipers in Ukraine, DynoWiper in Poland, fake job interviews	Spying on Ukraine and NATO; destruction mostly in Ukraine, once in Poland	Government for APT28 (US, Germany, CERT-UA, EU/UK sanctions); researchers for Sandworm
Other Russian services and groups: FSB-linked Turla and TA446, the Static Tundra cluster, APT29-linked UNC7005, Laundry Bear	STOCKSTAY, DarkSword, Polish energy intrusion, account takeover phishing, Zimbra email theft	Long-term intelligence collection; one destructive operation against industrial systems (Poland)	Government for Laundry Bear, the Signal and WhatsApp campaign, and the FSB 16th Centre (EU); researchers otherwise
Russia-aligned hacktivist fronts: NoName057(16), Z-Pentest, CARR, IT Army of Russia	Danish elections, La Poste, attacks on Israel, Quebec water plant, Ukrposhta	Cheap DoS attacks around elections and holidays; opportunistic access to exposed equipment	Denmark and Sweden tie such groups to Russian state services; Canada named NoName057(16); EU and UK sanctioned CARR members
Fronts of Iran's Ministry of Intelligence: Handala, Homeland Justice	Shamir hospital (per Israel), Stryker, Albanian Parliament, Patel leak, Clalit claim	Destructive attacks and leaks presented as hacktivism	Government (US DOJ, Albania's AKSK, Israel's cyber directorate)
Groups linked to the Revolutionary Guards: CyberAv3ngers lineage; IRGC propaganda network	US controller tampering; propaganda removed by Europol	Interference with industrial systems on the enemy's soil; wartime propaganda	Government (FBI-led advisory; Europol)
Other Iran-linked actors	Camera hijacking, Dust Specter, Jordan silos, CHOSEN BRICK, phone tracking	Reconnaissance for strikes, regional spying, repression of dissidents	Government for Jordan and CHOSEN BRICK; researchers otherwise
Hamas-linked groups	Ashen Lepus; possibly the fake rocket-alert app	Espionage against Arab governments	Researchers
United States	Caracas raid, start of the Iran war	Cyber and space effects as part of military operations	Self-acknowledged, without detail
Ukraine	Wildberries, drone-operator data, SkyNet claim	Disruption timed with drone strikes; leaks	Own claims only

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

Operator	Incidents in this Report	Typical Behavior	How Strong the Attribution Is
China-nexus groups and contractors	Singapore telecoms, UNC2814, Salt Typhoon in Norway and the UK, BeyondTrust and F5, Antino, Mustang Panda, AI-agent campaigns, Integrity Technology	Spying on telecoms and governments; zero-days in network and remote access products; contractors building tools	Government for Integrity Technology and Norway's Salt Typhoon finding; researchers otherwise
North Korea	Upbit, Drift, KelpDAO, Axios, DreamJob	Theft for revenue; attacks on developers and software supply chains	Researchers; South Korean investigators for Upbit
Unattributed	US water wave, Iranian banks, PDVSA, Lithuania, UK generator, Pakistani TV	Mostly disruption of services and controls	None public

By Type of Action

Action	Examples	What the Evidence Shows
Tampering with industrial controls	Poland, US Rockwell controllers, US water wave, Jordan silos, Quebec plants	Local, short effects; in one case, alarms and shutdown logic disabled; no grid or water system failed
Destroying IT systems	Stryker, Albanian Parliament, Sandworm wipers, Polish wipers	The biggest business impact; security software stopped the Polish wiper
Long-term espionage	Singapore, UNC2814, Salt Typhoon, Antino, Turla, Laundry Bear, Lithuania	Long presence inside networks, little visible effect, high intelligence value
Account and identity takeover	Signal and WhatsApp, UNC7005 and UNC5976, GRU routers	Normal features abused; encryption not broken
Psychological operations	BadeSaba, Iranian TV, Israeli station screens, Pakistani TV, mass text messages	Trusted channels hijacked within hours of strikes
Denial-of-service attacks	Denmark, La Poste, attacks on Israel, Azerbaijan, SkyNet	Hours of unavailability, no break-in
Supply chain and zero-days	F5, BeyondTrust, Axios, DarkSword	Very wide exposure; few named victims
Financial theft	Upbit, Drift, KelpDAO	Hundreds of millions of dollars, attributed to North Korea by researchers
Physical strikes on digital infrastructure	Kyiv data centers, Yandex, and Sberbank data centers	More disruption to everyday services than most cyberattacks

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Ways of Working

1. **Cyber as the first layer of a military operation.** The US described cyber and space effects as its opening move in Venezuela and Iran. Russia uses intrusions to plan and assess missile strikes in Ukraine. Ukraine paired a cyberattack with drone strikes on Wildberries. In no case has the public seen which systems were hit.
2. **States behind hacktivist masks.** Handala, Homeland Justice, and the Russia-aligned fronts give governments deniability. This period saw unusually many official statements pulling the masks off: the US on Iran's fronts, Denmark and Sweden on Russia-aligned groups, the EU and UK with sanctions.
3. **No malware needed.** The smaller Polish heat plant was stopped with normal controller commands, US controllers were changed with Rockwell's own software, and Stryker was wiped through Intune. Defenses that look only for malicious code miss attacks like these.
4. **Hiding in trusted cloud services.** Google Sheets, Outlook and OneDrive, Filen, and messaging apps carried attackers' commands. Blocking by website name does not stop this.
5. **Zero-days in the products defenders rely on.** F5, BeyondTrust, Zimbra, Office, iOS and the npm software registry were all exploited. Network edge and remote access devices remain the favorite way in for China-nexus groups.
6. **Getting in through someone else.** A supplier's VPN account opened the Albanian Parliament; leaked FortiGate settings and a mobile router opened Polish plants; another agency's accounts opened Lithuania's register.
7. **AI in the operator's chair.** GTG-1002 and the Taiwan campaign used AI agents for much of the intrusion work, and Sandworm and Dust Specter used AI to write code. The evidence is still thin: two reports by private companies and one government confirmation.
8. **The network itself as a weapon.** Iran cut its own population off for months. Russia and Ukraine bombed each other's data centers. Neither is a cyberattack, but both shape the digital side of war as much as hacking does.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

LevelBlue SpiderLabs

Appendix E: Claims That Are Still Unproven

These claims are often repeated but, as of late October 2026, are not supported by public evidence.



Claim	What Is Established
Iran was behind the summer attacks on US water utilities	No federal or state attribution. US officials quoted in the press call Iran the main suspect; investigators are also checking whether someone imitated Iran.
Iran shut down the UK generator	Press attribution only; the UK government confirmed the incident but named no one.
Russia stole Lithuania's register records	Prosecutors suspect a foreign state; none has been named.
Israel hijacked BadeSaba and Iranian TV	Nobody claimed it; Israeli involvement is reported but not confirmed.
A cyberattack caused the Caracas blackout on January 3	The US acknowledged cyber effects in general; the cause of the blackout is not established.
Sandworm alone carried out the Polish energy attack	CERT Polska points to the Static Tundra/Berserk Bear cluster, ESET to Sandworm; the service is disputed.
Handala wiped 200,000 Stryker devices and stole 50 TB	A source quoted by BleepingComputer put the wiped devices at nearly 80,000; the amount of stolen data is unverified.
Homeland Justice stole Albanian MPs' email	Albania's AKSK found the email server untouched; leaked files came from a file share.
Handala breached Clalit	Clalit said it was checking the claim; no confirmation found.
313 Team took down 1,825 Azerbaijani sites with 2.5 Tbps	Azerbaijan reported attacks on more than 100 domains, which kept running.
IT Army of Russia stole Ukrposhta's user database	Only the app outage is confirmed.
HUR (Ukrainian Intelligence) paralyzed Wildberries payments	Sellers reported delays; the scale is unverified.
BO Team disabled 15,000 SkyNet devices	SkyNet confirmed only a DoS attack.
Hijacked cameras guided specific Iranian strikes	Check Point shows targeted break-ins in areas under fire; use for any particular strike is inferred.
Iran tracked US troops' phones to target strikes	Based on an expert interview; no data published and no strike linked.
Salt Typhoon read British officials' messages	Press reports; the UK government has spoken only of "a cluster of activity."

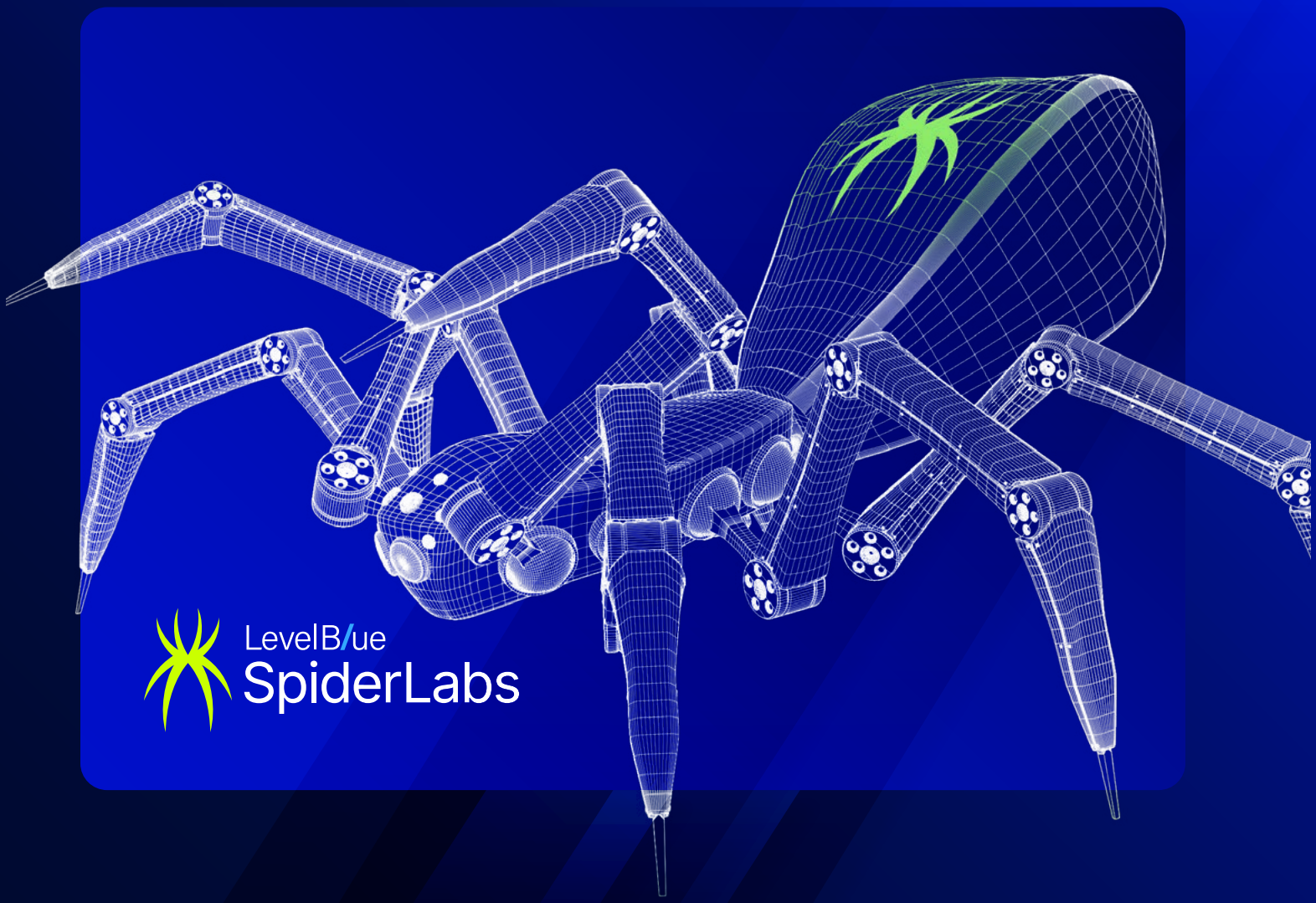
Coverage gaps. Sudan, the Thailand-Cambodia border conflict, the Sahel and most of the Caucasus produced mainly hacktivist claims or network outages without technical evidence, so no incident there met the standard of this report.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026



levelblue.com
levelblue.com/irr

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 6200-1 11-2026