Geopolitical Conflict as Cyber Escalation Catalyst

Nation-State and Hacktivist Wiper Campaigns Targeting Critical Infrastructure

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-26

Table of Contents

Nation-State and Hacktivist Wiper Campaigns Targeting Critical Infrastructure

Executive Summary

Two destructive cyberattacks separated by twelve days in March 2026 illustrate a pattern that security professionals can no longer treat as exceptional: when armed conflict erupts between major powers, enterprises throughout the global economy face an elevated and credible risk of deliberate data destruction, regardless of whether they are parties to the conflict. On March 11, 2026, the Iran-linked hacktivist group Handala claimed responsibility for wiping data from more than 200,000 devices belonging to Stryker Corporation, a $25 billion U.S. medical technology company operating in 61 countries — though this device count has not been independently verified and represents the attacker's own characterization [1]. On March 23, 2026, a financially motivated cybercriminal group called TeamPCP activated a geopolitically targeted wiper component within its CanisterWorm malware that specifically sought out and destroyed data on systems configured with Iran's timezone or Farsi locale settings [2]. The two attacks used entirely different actors, motives, and technical approaches, yet they arrived in the same two-week window — suggesting, though not conclusively establishing, that both were catalyzed by the same underlying geopolitical events. TeamPCP's motivation remains unattributed and is analyzed in detail below.

These incidents confirm that the threat surface for destructive cyber operations has expanded beyond military and government networks to encompass the global commercial enterprise. Critical infrastructure operators, defense contractors, healthcare companies, and multinational corporations with any perceived tie to conflicting parties now face a realistic probability of being targeted for data destruction by nation-state actors, state-affiliated hacktivist groups, and opportunistic criminals who weaponize geopolitical sentiment. More fundamentally, the March 2026 attacks demonstrate that wiper operations no longer require sophisticated malware on individual endpoints; the Stryker attack was accomplished by weaponizing enterprise device management infrastructure itself, wiping tens of thousands of devices with no malware deployed [3].

This whitepaper examines the strategic and technical dimensions of these campaigns in the broader historical context of wiper malware as a geopolitical instrument. It identifies the structural vulnerabilities that wiper campaigns exploit — particularly the management plane exposures that have become the preferred attack surface — and provides cloud security professionals with a framework for assessing and reducing their organization's exposure to geopolitically motivated destructive cyber operations.

Introduction: The New Geopolitical Cyber Equation

For most of the history of computer security, nation-state cyberattacks were understood as a concern primarily for governments, defense contractors, and critical infrastructure operators such as power utilities and water treatment facilities. The assumption held that most commercial enterprises occupied a kind of implicit neutrality in international cyber conflict — that hackers affiliated with foreign governments would largely pass over the accounts payable department of a medical device manufacturer in favor of targets with clear strategic value.

That assumption has been eroding for more than a decade, and the events of early 2026 demonstrate that organizations in any sector can no longer treat nation-state cyber risk as peripheral to their threat models. The modern geopolitical cyber equation has three components that collectively make commercial enterprises broadly vulnerable to destructive attacks as a consequence of conflicts they did not choose to be part of.

The first component is the deliberate targeting of civilians and civilian enterprises as instruments of political pressure. This approach is not new — coercive statecraft has always tried to impose costs on the civilian population or economy of an adversary — but its application through cyber means has become considerably more systematic. Groups like Handala, formally tied to Iran's Ministry of Intelligence and Security (MOIS), explicitly frame attacks on commercial enterprises in moral and political terms, identifying business relationships with governments they oppose as sufficient justification for destruction [4]. When Handala attacked Stryker, the group cited the company's approximately $450 million in U.S. Department of Defense contracts as the rationale, framing a medical device company as a legitimate target on the basis of its commercial dealings with the U.S. government [3].

The second component is the emergence of hacktivist groups that function as deniable, forward-deployed cyber forces. These groups exist at the intersection of state direction and independent action, allowing governments to pursue destructive objectives while maintaining a degree of plausible deniability. The ecosystem around armed conflict in the Middle East has generated a proliferation of such actors, ranging from groups with direct operational ties to Iranian and regional intelligence services to genuinely independent actors who are nonetheless inspired and coordinated by the conflict's emotional and political dynamics.

The third component is the expanding attack surface of cloud-managed enterprise infrastructure. The same centralized management planes that make large, globally distributed organizations governable — Microsoft Intune, AWS Systems Manager, Kubernetes cluster administrators — also represent significant single points of failure when compromised by a determined adversary, as the Stryker intrusion demonstrated. The March 2026 attack should be understood as a proof of concept that state-affiliated groups have internalized this reality and will exploit it.

Historical Context: Wiper Malware as Geopolitical Instrument

Destructive wiper malware — software designed to permanently destroy data rather than encrypt it for ransom — has been deployed as a geopolitical instrument for more than a decade. Understanding the historical trajectory of these attacks is essential for appreciating the significance of the 2026 campaigns.

The modern era of geopolitically motivated wiper malware effectively began in August 2012, when a group calling itself the "Cutting Sword of Justice" deployed Shamoon (also known as DistTrack) against Saudi Aramco, destroying approximately 30,000 workstations — at the time the most destructive cyberattack against a single organization [5, 6]. Shamoon overwrote the Master Boot Record of infected systems and replaced files with an image of a burning American flag, rendering machines permanently unbootable. Attribution pointed to Iranian state actors, and the attack was widely interpreted as Iran's response to international sanctions and sabotage operations against its own nuclear infrastructure. Shamoon returned in two subsequent campaign waves in 2016–2017 and again in 2018, each time targeting energy and critical infrastructure in Saudi Arabia and the wider Middle East.

The pattern of wiper attacks deploying alongside or in close temporal proximity to conventional military operations became definitively established in Eastern Europe. In December 2015 and again in December 2016, the Russian GRU-linked group Sandworm conducted the first confirmed cyberattacks to cause physical blackouts, using BlackEnergy and then Industroyer (also called CrashOverride) to knock out electrical power across portions of Ukraine [7]. Industroyer was the first malware specifically engineered to understand and manipulate industrial control system protocols for electrical grid equipment, capable of directly commanding circuit breakers and switches without relying on operator software.

Among the most financially damaging wiper attacks on record, the June 2017 NotPetya campaign arrived when Sandworm deployed destructive malware through a supply chain compromise of M.E.Doc, Ukrainian accounting software used by nearly all businesses operating in Ukraine [8]. Although styled after ransomware, NotPetya contained no decryption mechanism — it was designed exclusively to destroy. The malware spread globally within hours using the NSA-developed EternalBlue exploit and caused damages estimated in excess of $10 billion, with individual corporate losses including approximately $870 million at Merck, $400 million at FedEx's TNT subsidiary, $384 million at Saint-Gobain, and between $250 million and $300 million at Maersk [8]. The Maersk incident — in which the global shipping conglomerate lost 45,000 PCs, 4,000 servers, and 2,500 applications and was required to rebuild its entire global IT infrastructure in ten days — demonstrated conclusively that collateral damage from geopolitically targeted wiper attacks could devastate organizations with no meaningful connection to the underlying conflict.

The 2022 invasion of Ukraine generated the most prolific documented campaign of wiper malware in history, with researchers identifying at least nine distinct wipers deployed against Ukrainian and adjacent targets in rapid succession: WhisperGate, HermeticWiper, IsaacWiper, DesertBlade, AcidRain, CaddyWiper, DoubleZero, AwfulShred, and SoloShred [9]. AcidRain, deployed in the opening hours of the invasion to permanently destroy tens of thousands of Viasat KA-SAT satellite modems across Ukraine and Europe, demonstrated that wiper attacks could be precisely timed to coincide with and support conventional military objectives, disrupting Ukrainian military communications at the moment of maximum operational impact [10]. As collateral damage, AcidRain knocked out remote monitoring for approximately 5,800 wind turbines in Germany, illustrating again how geopolitically targeted destruction spills into unintended sectors and geographies [10].

This history establishes three enduring characteristics of geopolitically motivated wiper operations that provide essential context for interpreting the 2026 attacks. First, wiper attacks by state and state-affiliated actors have consistently targeted commercial enterprises alongside or instead of government and military infrastructure. Second, destructive operations are closely timed to kinetic military events, suggesting they function as components of broader coercive strategies. Third, the collateral damage radius of wiper attacks routinely extends far beyond the intended target, and organizations with no meaningful connection to the conflict can suffer severe losses.

The 2025–2026 Iran Conflict Cyber Theater

The geopolitical crisis that gave rise to both the Handala and CanisterWorm wiper operations began with Israeli and U.S. airstrikes against Iran in June 2025, a campaign variously referred to as the "Twelve-Day War." Security researchers documented a 700% increase in cyberattacks targeting Israeli infrastructure relative to pre-strike activity levels in the weeks following these strikes, with more than 600 distinct cyberattack claims appearing across over 100 Telegram channels within fifteen days of the kinetic operations [11, 12]. This surge established the pattern: kinetic military action catalyzes a rapid and measurable expansion of cyber operations against entities perceived as affiliated with either side of the conflict.

The situation escalated dramatically on February 28, 2026, when the United States and Israel launched coordinated airstrikes — designated Operation Epic Fury by U.S. forces and Operation Roaring Lion by Israel — targeting multiple sites across Iran. These strikes killed Iranian Supreme Leader Ali Khamenei and several senior officials [13]. The strikes also reportedly struck an Iranian school, with subsequent reporting by The New York Times determining that the United States bore responsibility for a Tomahawk missile strike that killed at least 175 people, most of them children [14]. Iran's internet connectivity collapsed to 1–4% of normal capacity in the immediate aftermath of the strikes, temporarily constraining the regime's ability to direct sophisticated centralized cyber operations [13]. Intelligence assessments concluded that this connectivity

disruption would mitigate the most sophisticated state-directed attacks in the near term, while geographically dispersed operators — including those already positioned outside Iran — could sustain lower-sophistication but still disruptive campaigns [12].

The threat landscape at the time included a diverse ecosystem of actors. Handala (Void Manticore, MOIS-affiliated) was conducting operations against Israeli energy infrastructure, Jordanian fuel systems, and Israeli healthcare networks. APT42 (also known as RedKitten) was running macro-document campaigns against human rights NGOs. CyberAv3ngers, an IRGC-affiliated group, continued targeting operational technology infrastructure in U.S. and Israeli water utilities. The Canadian Centre for Cyber Security issued a formal threat bulletin in early March 2026 warning organizations to expect Iranian cyber responses to the U.S./Israel strikes, identifying critical infrastructure, government networks, and entities with defense industry ties as the most likely targets [15].

Two developments in early March 2026 transformed this elevated-but-diffuse threat environment into concrete, high-consequence attacks against commercial enterprises. The first was the Stryker intrusion, claimed on March 11 by Handala. The second was the activation of CanisterWorm's geopolitical wiper payload through a supply chain attack on March 19, with the wiper campaign becoming publicly known on March 23.

Case Study: Handala's Attack on Stryker Corporation

Background and Attribution

Stryker Corporation is a global medical technology company headquartered in Kalamazoo, Michigan, reporting approximately $25 billion in annual sales and employing roughly 56,000 people across 61 countries [1]. The company manufactures a broad range of medical and surgical equipment, including orthopedic implants, surgical instruments, neurotechnology, and emergency medical equipment. Stryker maintains approximately $450 million in U.S. Department of Defense contracts [3].

The group that claimed responsibility, Handala (also known as Handala Hack Team), is a public-facing operational persona for Void Manticore, a destructive cyber unit embedded within Iran's MOIS, specifically its Counter-Terrorism Division [4]. The group's name derives from a well-known Palestinian political cartoon character by artist Naji al-Ali, carrying deliberate symbolic weight. The MOIS connection was confirmed through investigation by researchers at Check Point Research and others, who tied the unit to the MOIS Counter-Terrorism Division led by Seyed Yahya Hosseini Panjaki, a deputy minister sanctioned by the U.S. Treasury Department in September 2024 and subsequently sanctioned by the EU and UK [4]. Palo Alto

Networks has profiled Handala as one of several personas maintained by Void Manticore, noting that the group surfaced in late 2023 and represents an escalating progression from intelligence collection toward destructive operations [1].

Handala's operational history prior to Stryker was concentrated on Israeli and Albanian targets. The group conducted multiple destructive intrusions against Albanian government infrastructure under the persona "Homeland Justice" beginning in 2022, and subsequently shifted toward a campaign combining hack-and-leak operations with data destruction against Israeli political, defense, and civilian organizations. One particularly notable operation in January 2026 compromised emergency alert systems at over twenty Israeli kindergartens, forcing activation of air raid sirens and broadcasting threatening messages — an operation designed for maximum psychological impact against civilians [4].

Mechanics of the Attack

On March 11, 2026, Handala posted a lengthy statement to Telegram claiming responsibility for a global cyberattack against Stryker, asserting that the group had erased data from more than 200,000 systems, servers, and mobile devices, forcing Stryker to shut down offices across 79 countries [1]. Stryker has not publicly confirmed the scale of the breach, and as of this writing the 200,000-device claim remains the attacker's unverified self-report. The Krebs on Security report from that day described employees in Ireland — one of Stryker's largest hubs outside the United States — being sent home after systems went dark, with those who had Microsoft Outlook on personal phones finding their personal devices wiped as well [1]. Stryker's own phone system confirmed that the company was experiencing a "building emergency."

Initial reporting assumed Handala had deployed wiper malware in the manner of previous destructive operations. Subsequent investigation revealed something more significant: the attack required no malware deployed on individual endpoints at all. Handala had gained access to Stryker's Microsoft Intune instance — the enterprise mobile device management (MDM) and endpoint management platform that Stryker used to manage its global device fleet — and issued a Remote Wipe command through the management infrastructure itself, simultaneously triggering device wipes across the organization's global footprint [3]. Stryker later confirmed it found no evidence of malware or ransomware deployed on individual systems.

The implications of this methodology deserve careful attention. Intune, and enterprise management platforms like it, exist precisely to give IT administrators centralized authority over organizational devices at global scale. The same capability that enables legitimate remote wipe of a lost laptop becomes, when accessed by an adversary, a weapon capable of simultaneously destroying data on every managed device in the organization. The management plane had become the weapon.

Handala also claimed to have exfiltrated approximately 50 terabytes of data from Stryker's systems prior to initiating the wipe. While this claim has not been independently verified, it is consistent with Void Manticore's documented pattern of combining data theft with destruction to create dual coercive leverage —

threatening both operational disruption and public disclosure of sensitive information [3].

Stated Motivation and Strategic Logic

Handala publicly justified the attack by citing Stryker's U.S. Department of Defense contracts, framing the company as a defense industry participant rather than a civilian healthcare provider. The Handala statement, posted to Telegram, specifically linked the attack to the February 28 missile strike on an Iranian school and declared it retaliation for what the group characterized as the murder of children [1]. Handala stated: "All the acquired data is now in the hands of the free people of the world, ready to be used for the true advancement of humanity and the exposure of injustice and corruption" [1].

This framing reflects the strategic logic of state-affiliated hacktivist operations: create coercive costs for entities perceived as complicit in the adversary's military actions, generate psychological pressure on the civilian population, and produce narrative content that can be amplified through information operations. The selection of a medical technology company with defense contracts rather than a purely military or governmental target also reflects an apparent evolution in Handala's targeting doctrine — an expansion from the infrastructure and government targets typical of state-directed cyber operations toward the broader category of private enterprises with commercial ties to the adversary government.

Law Enforcement Response

On March 19, 2026 — eight days after the Stryker attack — the FBI seized Handala's websites and associated domains, announcing domain seizures linked to the Iranian hacker group [16]. The Justice Department's action confirmed the seriousness with which U.S. law enforcement viewed the Stryker incident and continued the pattern of U.S. government disruption operations against Iranian cyber personas following major attacks on U.S. entities.

Case Study: CanisterWorm's Geopolitically Targeted Wiper

TeamPCP Background

TeamPCP (also tracked under the aliases DeadCatx3, PCPcat, ShellForce, and CanisterWorm) is a financially motivated cybercriminal group that emerged as a significant cloud security threat in December 2025 [17]. Unlike state-sponsored actors, TeamPCP's primary objectives are credential theft, data exfiltration, and extortion through Telegram. What distinguishes the group from traditional cybercriminal

operations is its almost exclusively cloud-native attack methodology. In a January 2026 profile published by the security firm Flare, researcher Assaf Morag characterized the group's strength as arising "not from novel exploits or original malware, but from the large-scale automation and integration of well-known attack techniques," adding that "the group industrializes existing vulnerabilities, misconfigurations, and recycled tooling into a cloud-native exploitation platform that turns exposed infrastructure into a self-propagating criminal ecosystem" [2, 17].

TeamPCP's attack surface consists of exposed cloud control planes: Docker APIs left accessible without authentication, Kubernetes cluster management interfaces exposed to the internet, Redis servers accessible without credentials, and CI/CD pipeline secrets stored in plaintext. With Azure environments accounting for approximately 61% of TeamPCP's compromised servers and AWS for 36%, the group's victims span nearly the entirety of enterprise cloud infrastructure [2].

The Trivy Supply Chain Compromise

On March 19, 2026, TeamPCP executed a supply chain attack against Trivy, the open-source container security scanner maintained by Aqua Security and among the most widely used vulnerability scanning tools in cloud-native environments [2, 18]. The attack targeted Trivy's GitHub Actions CI/CD workflows, injecting a credential-stealing payload into official releases. Organizations that downloaded affected Trivy releases inadvertently exposed SSH keys, cloud credentials, Kubernetes service account tokens, and cryptocurrency wallet data to attacker-controlled infrastructure [2].

The supply chain attack proved to be a pivot point. Within days, Sysdig researchers observed the same "TeamPCP Cloud Stealer" appearing in workflows belonging to Checkmarx, a supply chain security company whose KICS (Keeping Infrastructure as Code Secure) GitHub Actions were compromised using credentials stolen in the Trivy attack [19]. Security researchers at Endor Labs simultaneously identified that litellm, a widely used Python library for interacting with large language model APIs, had been backdoored in versions 1.82.7 and 1.82.8 published on March 24, 2026 — again via the Trivy CI/CD infection chain [20]. The cascade demonstrated how a single supply chain foothold could rapidly propagate across an interconnected ecosystem of open-source tooling.

The CanisterWorm Wiper: Geopolitical Targeting Logic

The CanisterWorm malware takes its name in part from its command-and-control infrastructure architecture: rather than using conventional servers or domain-based C2, the malware communicates through Internet Computer Protocol (ICP) canisters — blockchain-based smart contracts that are architecturally resistant to law enforcement seizure or traditional takedown operations [2]. This design decision suggests meaningful operational security investment on TeamPCP's part.

In the same timeframe as the Trivy supply chain attack, security researcher Charlie Eriksen at Aikido documented a new wiper payload deploying through the same technical infrastructure [2]. The payload's targeting logic was explicit and geopolitical: when executed, CanisterWorm evaluates whether the host system's timezone matches `Asia/Tehran` or whether the system locale is configured as `fa_IR` (Farsi). For systems that satisfy these conditions and have access to a Kubernetes cluster, the malware deploys a DaemonSet named `host-provisioner-iran` to the `kube-system` namespace. This DaemonSet runs an Alpine container named "kamikaze" with privileged access and the host root filesystem mounted at `/mnt/host`, deleting all top-level directories and forcing a system reboot [2]. On standalone Linux hosts without Kubernetes access, the malware uses the `shred` and `rm` utilities to overwrite and delete files. For systems that do not match the Iranian geolocation criteria, the payload installs persistence tooling rather than destroying data — a binary outcome determined entirely by the victim's geographic configuration.

The deliberate targeting of Iranian systems by a financially motivated criminal group represents an unusual convergence of criminal and geopolitical interests. Charlie Eriksen assessed the motivation as potentially "chaotic evil," acknowledging that the Iran targeting could represent genuine geopolitical involvement, nation-state contracting, or attention-seeking behavior by a criminal actor attempting to align with conflict sentiment [2]. No public attribution to a specific government sponsor had been made as of this writing. What is clear is that the same infrastructure and tooling used to steal credentials from cloud environments globally was repurposed, in the same campaign window, to execute geopolitically targeted data destruction against a specific national population — demonstrating that the threshold for a financially motivated group to engage in geopolitically motivated destruction may be considerably lower than previously assumed.

The Management Plane as Weaponized Attack Surface

The Stryker intrusion introduces a threat vector that cloud security professionals must treat as a first-tier risk: the enterprise management plane as a vector for mass destruction. This is not a novel theoretical concern — the ability of enterprise management platforms to perform remote wipe operations at scale has been documented in security literature for years. What the Stryker attack demonstrates is that state-affiliated groups have clearly incorporated management plane exploitation into their destructive playbooks, and that once an adversary has authenticated to an Intune tenant as a privileged administrator, the time between issuing a Remote Wipe command and mass device destruction across a global fleet can be measured in minutes.

The management plane encompasses a range of services and platforms. Microsoft Intune and Endpoint Configuration Manager provide enrollment, policy management, and remote wipe capabilities for Windows, macOS, iOS, and Android devices. AWS Systems Manager enables remote command execution across EC2

instances at scale. Google Workspace admin consoles and Microsoft 365 admin centers can provision, reconfigure, and revoke access to user accounts and data. Kubernetes cluster administrator credentials provide root-equivalent access to all workloads and data on every node in the cluster. In each case, the platform's legitimate administrative power — the reason organizations adopt these tools — is functionally identical to the destructive power an adversary wields upon gaining access.

The CanisterWorm Kubernetes wiper component illustrates this from the cloud-native direction. Kubernetes cluster administrator access is the prerequisite for deploying the `host-provisioner-iran` DaemonSet that destroys every node in the cluster. Kubernetes service account tokens stolen from CI/CD environments — the exact credential class captured in the Trivy supply chain attack — frequently carry cluster-admin-equivalent privileges in organizations that have not implemented least-privilege role-based access control policies. The attack chain therefore runs directly from supply chain compromise to credential theft to management plane access to mass destruction.

This architecture creates a category of attack where the technical sophistication required to achieve catastrophic impact is considerably lower than the damage scale might suggest. An attacker who can authenticate to an Intune tenant as a privileged administrator, or who can obtain cluster-admin credentials for a large Kubernetes deployment, does not need to understand the internal architecture of every system they subsequently destroy. The management infrastructure handles that complexity. Security programs that focus defensive investment primarily on endpoint security, perimeter defenses, and network monitoring while treating identity and access management for administrative platforms as a lower priority have their risk calculus fundamentally inverted relative to this threat model.

The Hacktivist–Nation-State Nexus

Both the Handala and CanisterWorm cases illustrate distinct expressions of a broader phenomenon: the increasingly complex relationship between criminal, hacktivist, and nation-state actors in geopolitically motivated cyber operations. Understanding this nexus is essential for accurate threat modeling.

Handala exemplifies what Check Point Research has called "faketivist" operations: groups that maintain a genuine hacktivist identity and messaging, and that may include individuals with authentic political commitments, while operating under the organizational umbrella and operational direction of an intelligence agency [4]. The MOIS direction of Void Manticore, the organizational structure behind Handala, is assessed with high confidence by Check Point Research, Palo Alto Networks Unit 42, and others, yet Handala's public communications adopt the tone and framing of an independent hacktivist collective making autonomous political decisions [1, 4]. This ambiguity serves multiple functions simultaneously: it provides the Iranian

government with plausible deniability, it amplifies the attack's psychological and informational impact through hacktivist framing, and it makes traditional law enforcement responses — which depend on prosecutable individual actors — more complex to execute.

Palo Alto Networks' analysis of the broader ecosystem in the weeks following Operation Epic Fury documented a wide spectrum of actor sophistication and state affiliation operating concurrently: highly capable MOIS-directed groups like Void Manticore conducting strategic, targeted operations; IRGC-affiliated groups like CyberAv3ngers continuing persistent campaigns against operational technology infrastructure; genuinely independent hacktivist groups conducting lower-sophistication defacement and DDoS operations in response to the conflict's emotional dynamics; and criminal actors like TeamPCP potentially leveraging geopolitical sentiment as either cover or genuine motivation for destructive operations that serve dual commercial and political ends [12].

This spectrum complicates the enterprise risk calculus in a specific way: organizations cannot confine their concern to sophisticated, state-directed attacks for which attribution and warning intelligence typically exist. The range of actors motivated to conduct destructive operations expands dramatically whenever a major geopolitical event activates this ecosystem, and the technical quality of attacks varies across a wide range. A medium-sophistication attack exploiting a misconfigured Kubernetes cluster by an actor motivated entirely by geopolitical sentiment may produce the same operational impact as a sophisticated, state-directed intrusion — and may arrive without the intelligence indicators that typically precede the latter.

Threat Actor Taxonomy: Current Geopolitically Motivated Wiper Actors

The following table summarizes the principal threat actors conducting or enabling geopolitically motivated wiper or destructive operations relevant to the current Iran-related conflict context. This taxonomy is based on public intelligence as of March 2026.

Actor	State Affiliation	Primary Targets	Destructive Capability	Key TTPs
Handala (Void Manticore)	MOIS (Iran)	Israel, U.S. defense industry, Western enterprises	High — mass wiper deployment via MDM/management plane	VPN credential theft, Intune compromise, BiBi wiper, VeraCrypt, Group Policy deployment

Actor	State Affiliation	Primary Targets	Destructive Capability	Key TTPs
CyberAv3ngers	IRGC (Iran)	Water utilities, OT/ICS infrastructure, Israel	High – SCADA/PLC targeting	IOControl malware, industrial protocol exploitation
APT42 (RedKitten)	IRGC (Iran)	NGOs, dissidents, Western targets	Low-medium – primarily espionage with disruptive potential	Macro documents, GitHub/Google Drive C2
FAD Team	Iran-aligned	SCADA/PLC industrial systems	High – permanent OT destruction	Wiper malware targeting ICS protocols
TeamPCP	Criminal (unattributed)	Cloud infrastructure globally, Iran (wiper)	High for Iranian targets – blockchain C2, Kubernetes DaemonSet wiper	Supply chain compromise, CI/CD poisoning, ICP-based C2
Sandworm	GRU (Russia)	Ukraine, Europe, global collateral	Very high – Industroyer2, CaddyWiper, AcidRain	ICS protocol manipulation, satellite infrastructure

Organizational Risk Assessment Framework

Enterprises seeking to evaluate their exposure to geopolitically motivated wiper operations should structure their assessment around three dimensions: targeting logic, attack surface, and organizational resilience.

Targeting Logic. Wiper campaigns exhibit a range of targeting selectivity, from the broad geolocation-based destruction of CanisterWorm to the specific enterprise selection of the Handala-Stryker attack. Organizations should assess whether they possess characteristics that make them likely targets of politically motivated destruction: contracts with government entities at the center of a conflict, a national headquarters or significant operational presence in a country that is the subject of attack, publicly stated

policy positions or affiliations, or visible commercial relationships with entities that adversary groups have publicly designated as targets. This assessment should be updated regularly as geopolitical conditions evolve, because the list of "relevant" affiliations expands rapidly during periods of active conflict.

Attack Surface. The key attack surface categories most relevant to wiper operations are management plane identity and access controls, CI/CD pipeline security, and cloud credential exposure. Organizations should specifically audit which administrators can perform remote wipe operations at scale on their endpoint fleet, what authentication and authorization controls protect that capability, and whether those controls would withstand a credential theft attack. The same audit should be applied to Kubernetes cluster administrator roles and cloud provider root or privileged access. Supply chain exposure through CI/CD tooling — the vector exploited in CanisterWorm's initial propagation — deserves specific attention for organizations using widely adopted open-source tools in their build pipelines.

Organizational Resilience. The ultimate test of a wiper attack is whether the organization can recover. Organizations should assess their backup architecture against a worst-case scenario in which every managed endpoint is simultaneously wiped, including mobile devices. Backup configurations that rely on management infrastructure to initiate or verify backups may be compromised simultaneously with the data they protect. Offline, immutable, and geographically isolated backup copies that cannot be reached through the same management plane as the production environment represent the minimum standard for organizations that take this threat seriously.

Conclusions and Recommendations

The March 2026 wiper campaigns confirm that commercial enterprises — including those in sectors historically considered peripheral to nation-state cyber operations — now face credible risk of deliberate data destruction as a consequence of geopolitical events they do not control and may not be aware of. The strategic logic driving this expansion of targets is not likely to reverse: geopolitically motivated actors have learned that attacking commercial enterprises creates broader coercive pressure and generates significant informational value, while enterprises in the post-cloud era present a management plane attack surface that makes mass data destruction feasible even for actors without sophisticated endpoint malware capabilities.

Immediate Actions

Organizations operating in or with significant commercial ties to geopolitically active regions should conduct an immediate audit of their enterprise management plane security posture. This audit should address authentication strength and MFA configuration for all Intune, Systems Manager, Workspace, and similar administrative interfaces; the scope of remote wipe capabilities available to compromised administrator accounts; and whether management plane access logging is configured and reviewed. Any service accounts

associated with CI/CD pipelines — particularly those with access to Kubernetes cluster administrator privileges — should be treated as high-value credential targets and protected accordingly, including rotation of credentials already present in any CI/CD systems that use widely shared open-source tools such as Trivy.

Organizations should verify that backup configurations produce recoverable copies that are isolated from the management plane. Specifically, mobile device and endpoint backup configurations should be reviewed to ensure that a Remote Wipe command affecting enrolled devices does not simultaneously erase backup copies accessible through the same administrative interface. The Stryker incident, in which personal employee devices with corporate email were wiped alongside corporate-managed endpoints, suggests that organizations should also evaluate the scope of MDM enrollment policies and whether personal devices with access to corporate data should be enrolled in the same management domain as corporate assets.

Short-Term Mitigations

Over the following thirty to ninety days, organizations should implement or verify Privileged Identity Management (PIM) and Privileged Access Management (PAM) controls for management plane administrative roles, ensuring that high-privilege actions — including mass remote wipe — require just-in-time approval and cannot be performed continuously from a standing privileged session. Organizations that have not yet implemented phishing-resistant multi-factor authentication (such as FIDO2 hardware keys or device-bound passkeys) for management plane access should treat this as a critical priority; the initial access vectors for Handala operations have historically included VPN credential theft, and credential-based initial access remains the most common path to management plane compromise.

On the cloud infrastructure side, organizations using Kubernetes should audit role bindings to ensure that CI/CD service accounts and externally exposed tokens do not carry cluster-admin or equivalent privileges. The principle of least privilege is frequently honored in abstract security policy but violated in practice in CI/CD configurations; this gap creates exactly the attack path that TeamPCP exploited. Kubernetes audit logging should be enabled and monitored for anomalous DaemonSet deployments, particularly those targeting `kube-system` with privileged host-path volume mounts.

Supply chain hygiene for CI/CD tooling should be implemented through pinning official container image digests rather than tags, cryptographic verification of pipeline tool integrity where available, and monitoring for unexpected changes to CI/CD workflow files in source control. The Trivy supply chain compromise was possible in part because many organizations' build pipelines consume external tooling without validation mechanisms that would detect substitution of malicious versions.

Strategic Considerations

At the strategic level, enterprises that have not yet developed geopolitical threat intelligence capabilities should consider how they will receive and integrate warning about elevated threat environments into their security operations. The Canadian Centre for Cyber Security issued a threat bulletin in early March 2026 warning of elevated Iranian cyber threat activity; organizations with effective intelligence functions would have used that warning to activate elevated monitoring and apply enhanced controls to management plane access in the days before the Stryker attack. The gap between geopolitical event and organizational security response needs to be measured in hours, not weeks.

Organizations should also invest in tabletop exercises specifically designed around the management plane wiper scenario — exercises in which the scenario is not "ransomware has encrypted our file servers" but "our Intune tenant was compromised and a Remote Wipe command was issued to every enrolled device at 3:00 AM." The recovery procedures required for this scenario are substantially different from traditional ransomware recovery, and the organizational decision-making challenges — particularly around personal devices enrolled in corporate MDM — are not well-addressed by most incident response plans.

Finally, organizations with significant exposure to geopolitically active sectors or regions should engage with sector-specific information sharing organizations (ISACs) and government threat sharing programs as a sustained practice rather than a reactive one. The pace at which threat intelligence about Handala's operations, TeamPCP's CI/CD attack chain, and the broader Iranian cyber threat landscape was shared among security vendors and governments in the weeks following February 28, 2026, demonstrates that this ecosystem of sharing functions; the gap is frequently on the receiving end, where organizations have not established the channels or processes to receive and act on shared intelligence rapidly.

CSA Resource Alignment

The Cloud Security Alliance has published guidance directly relevant to the organizational vulnerabilities exposed by the March 2026 wiper campaigns. The following resources provide specific frameworks and controls applicable to the attack vectors and response requirements identified in this paper.

Cloud Incident Response Framework. CSA's Cloud Incident Response Framework [21] provides the foundational methodology for preparing for and responding to destructive incidents of the type described in this paper. The framework's emphasis on pre-incident preparation — including documented recovery procedures, tested backups, and defined roles for cloud-specific response scenarios — applies directly to the management plane wiper scenario. The Stryker intrusion's most damaging dimension was not the attack itself but the absence of recovery procedures designed for simultaneous global device destruction;

organizations should review their incident response plans against the framework's requirements specifically for destructive incidents, which present different recovery challenges than confidentiality or availability incidents.

CSA Medical Device Incident Response Playbook. CSA has published a specific incident response playbook for medical device organizations [22], directly applicable to the Stryker scenario and to the broader class of healthcare and medtech enterprises that have become targets of geopolitically motivated attacks. The playbook addresses the particular regulatory, patient safety, and operational continuity requirements of the medical technology sector — requirements that make the Handala attack pattern particularly consequential for this industry.

Cloud Threat Modeling (2025). CSA's cloud threat modeling guidance [23] provides the methodology for systematically identifying and evaluating cloud-specific attack paths, including the management plane attack surface that proved decisive in the Stryker intrusion. Organizations that have not applied structured threat modeling to their cloud management infrastructure — including MDM platforms, cloud provider administrative roles, and Kubernetes cluster access — should treat this as an urgent gap. The management plane compromise at Stryker is precisely the attack pattern that a well-executed cloud threat modeling exercise would identify as a catastrophic risk scenario warranting dedicated controls.

Zero Trust Guidance. CSA's Zero Trust publications [24] provide the security architecture framework for addressing the management plane access control failures that enabled both campaigns analyzed in this paper. The core Zero Trust principle — that no actor should be trusted by default based on network position or credential possession, and that all access should be continuously verified and minimally scoped — applies directly to the Intune compromise vector. The just-in-time and just-enough-access patterns described in CSA's Zero Trust guidance for privileged access align precisely with the control gaps that Handala exploited, where standing administrator credentials provided immediate global wipe capability.

AI Controls Matrix (AICM) and CCM. CSA's AI Controls Matrix [25], a superset of the Cloud Controls Matrix, addresses control requirements for cloud services and AI workloads. The CI/CD supply chain attacks executed by TeamPCP are directly relevant to controls addressing supply chain integrity, CI/CD pipeline security, and the management of trusted execution environments for automated systems. Organizations that have adopted the AICM as their cloud security control framework should ensure that supply chain controls in that framework are implemented for build tooling, not only for application dependencies — the Trivy compromise illustrates how security tooling in the build pipeline is itself an attack surface.

MAESTRO Framework. As AI-assisted security operations and AI-augmented threat actor capabilities become more prevalent in the conflict environment, CSA's MAESTRO framework for agentic AI threat modeling [26] provides relevant guidance. The potential for adversaries to use AI-assisted attack tooling to accelerate supply chain discovery, credential analysis, and lateral movement in cloud environments represents an emerging dimension of the threat described in this paper.

References

[1] Krebs on Security. "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker." March 11, 2026. https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/

[2] Krebs on Security. "'CanisterWorm' Springs Wiper Attack Targeting Iran." March 23, 2026. https://krebsonsecurity.com/2026/03/canisterworm-springs-wiper-attack-targeting-iran/

[3] Bleeping Computer. "Stryker Attack Wiped Tens of Thousands of Devices, No Malware Needed." March 2026. https://www.bleepingcomputer.com/news/security/stryker-attack-wiped-tens-of-thousands-of-devices-no-malware-needed/

[4] Check Point Research. "Handala Hack: Unveiling Group's Modus Operandi." March 12, 2026. https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/

[5] ICS-CERT. "ICS-CERT Alert: Shamoon Malware Targeting Energy Sector." August 2012. https://www.cisa.gov/news-events/ics-alerts/ics-alert-12-225-01

[6] Kaspersky Lab. "Shamoon the Wiper – Copycats at Work." August 2012. https://securelist.com/shamoon-the-wiper-copycats-at-work/57854/

[7] Dragos Inc. "CrashOverride: Analyzing the Malware that Attacks Power Grids." June 2017. https://www.dragos.com/resources/whitepaper/crashoverride-analyzing-the-malware-that-attacks-power-grids/

[8] Wired. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." August 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[9] CISA / NSA / FBI. "Advisory: Destructive Malware Targeting Organizations in Ukraine." February 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

[10] SentinelOne. "AcidRain: A Modem Wiper Rains Down on Europe." March 2022. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

[11] Radware. "700% Increase in Cyberattacks Against Israeli Infrastructure Following Airstrikes." June 2025. https://www.radware.com/resources/threat-intelligence/

[12] Palo Alto Networks Unit 42. "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran." March 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

[13] SOCRadar. "Iran vs. Israel and US Cyber War 2026: Operation Epic Fury." March 2026. https://socradar.io/blog/cyber-reflections-us-israel-iran-war/

[14] The New York Times. "U.S. Strike Killed 175 in Iran, Most of Them Children, Investigators Find." March 2026. [URL not available at time of publication]

[15] Canadian Centre for Cyber Security. "Cyber Threat Bulletin: Iranian Cyber Threat Response to US/Israel Strikes." March 2, 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026

[16] TechCrunch. "FBI Seizes Pro-Iranian Hacking Group's Websites After Destructive Stryker Hack." March 19, 2026. https://techcrunch.com/2026/03/19/fbi-seizes-pro-iranian-hacking-groups-websites-after-destructive-stryker-hack/

[17] Flare. "TeamPCP: Industrializing Cloud Exploitation." Assaf Morag. January 2026. https://flare.io/learn/resources/blog/teampcp-cloud-exploitation/

[18] Aikido Security. "CanisterWorm: When a Security Scanner Becomes a Wiper." Charlie Eriksen. March 23, 2026. https://www.aikido.dev/blog/canisterworm-when-a-security-scanner-becomes-a-wiper

[19] Sysdig. "TeamPCP Cloud Stealer: Trivy Compromise Spreads to Checkmarx KICS." March 2026. https://sysdig.com/blog/teampcp-cloud-stealer-trivy-checkmarx/

[20] Endor Labs. "TeamPCP Isn't Done: LiteLLM Supply Chain Attack Analysis." March 24, 2026. https://www.endorlabs.com/learn/teampcp-isnt-done

[21] Cloud Security Alliance. "Cloud Incident Response Framework." https://cloudsecurityalliance.org/research/cloud-incident-response-framework

[22] Cloud Security Alliance. "CSA Medical Device Incident Response Playbook." https://cloudsecurityalliance.org/research/medical-device-incident-response-playbook

[23] Cloud Security Alliance. "Cloud Threat Modeling 2025." https://cloudsecurityalliance.org/research/cloud-threat-modeling-2025

[24] Cloud Security Alliance. "Zero Trust Guidance." https://cloudsecurityalliance.org/research/zero-trust

[25] Cloud Security Alliance. "AI Controls Matrix (AICM)." https://cloudsecurityalliance.org/research/ai-controls-matrix

[26] Cloud Security Alliance. "MAESTRO: Agentic AI Threat Modeling Framework." https://cloudsecurityalliance.org/research/maestro