Estimating the Societal Cost of DDoS Attacks:

A Dual-Lens Model for National Impact Assessment

GFCE Discussion paper | July 2025

Written by

Carlos Álvarez, Director of the Americas & Caribbean Hub

GFCE
AMERICAS &
THE CARIBBEAN
HUB

Estimating the Societal Cost of DDoS Attacks: A Dual-Lens Model for National Impact Assessment[1]

Executive Summary

The July 2025 disruption of NoName057 through Operation Eastwood exposed a structural blind spot in how we assess the impact of DDoS campaigns. As coordinated operations that exploit institutional inertia, trigger overextended response cycles, and generate pressure at the national level without crossing traditional escalation thresholds, they must not be understood as isolated technical incidents or as mere nuisances.

Between February 2023 and July 2025, over 300,000 DDoS attacks were launched by this network and its affiliates. The majority targeted Ukraine and its allies, but the operational logic behind them was broader: to generate cumulative friction, force reactive resource allocation, and signal capability without attribution. In other words, weaponization of low-cost disruption at scale, with tangible effects on public confidence, state capacity, and international perception.

Frequently, this type of attacks is treated as nuisance-level bandwidth spikes. That approach, however, misses a way to assess societal impact in a way that reflects both the measurable and the strategic, that is, both what we can count and what we can't afford to ignore.

This paper introduces a dual-lens model designed for national-level application. On one axis, it quantifies financial and operational costs using attack volume, duration, and mitigation data. On the other, it scores the strategic and social effects that manifest through public disruption, institutional fatigue, and reputational damage. This approach supports decisions about prioritization, funding, and resilience, and helps national leadership communicate cyber threats in a language that resonates beyond the technical community.

The ultimate goal of this paper is to spark dialogue between governments, academia, civil society, the private sector and other relevant stakeholders around a proposed model to estimate the overall societal cost of DDoS attacks, through which capacity-building needs can be identified and prioritized, whether in the form of legislative reform, law enforcement training, international coordination, or public-private partnership development.

We started to work on this document on July 19, 2025, a few days after the law enforcement action against NoName057. We note that targeting through DDoSIA paused on 15 July and resumed on 23 July, and a few hours later the TLP of the attack logs was downgraded to Clear, after which they were posted to Silas Cutler's GitHub. Big thank you to Silas and others involved in production for allowing us TLP:Amber access to the full historical logs in advance of their publication.

Introduction

In a significant law enforcement action dubbed Operation Eastwood, a Europol and Eurojust-coordinated international operation successfully dismantled the pro-Russian cybercrime network NoName057 between July 14 and 17, 2025. This operation, involving raids in 12 countries, led to arrests in France and Spain, and the disruption of an attack infrastructure consisting of over one hundred computer systems worldwide, with a major part of the group's central server infrastructure taken offline. Seven international arrest warrants were issued, including six for suspects residing in the Russian Federation, two of whom are believed to be the principal organizers of the group's activities. Authorities also informed approximately 1100 supporters and 17 administrators about the measures taken and their criminal liability for their actions. NoName057 was responsible for thousands of distributed denial-of-service (DDoS) attacks targeting Ukraine and its allies, particularly critical infrastructure such as electricity suppliers and public transport systems across Europe.

The emergence of ideologically motivated cyber collectives like NoName057 has fundamentally altered the threat landscape through persistent, distributed cyber disruption campaigns. Leveraging tools such as DDoSIA, these operations enable low-cost, high-volume cyber attacks that generate cascading digital disturbances across critical sectors. Our analysis of all attack logs spanning February 2023 to July 2025 covers 304,659 attacks and reveals that while individual DDoS attacks may appear tactically limited, their aggregate societal impact remains substantially underestimated by traditional assessment frameworks.

This article presents a comprehensive model for evaluating the true societal cost of coordinated DDoS campaigns, integrating both measurable economic impacts and strategic consequences that transcend monetary quantification. The model distinguishes between:

- **Quantitative (Monetary) Costs**: Direct financial impacts that can be measured and budgeted.
- **Qualitative (Strategic and Social) Impacts**: Contextual effects on national stability, public trust, and geopolitical standing.

This dual-lens approach enables governments, security analysts, and institutions to comprehensively evaluate the full operational footprint of disruptive campaigns on national resilience and democratic stability.

1. The Strategic Significance of DDoSIA Operations

DDoSIA represents a paradigm shift in hacktivist operations, enabling volunteer-coordinated digital disruption campaigns orchestrated through encrypted communication platforms. NoName057's deployment of this infrastructure has systematically targeted governmental institutions, financial systems, transport networks, media outlets, and electoral infrastructure across 29 countries.

Our analysis reveals that dismissing these operations as mere nuisance attacks fundamentally misunderstands their strategic purpose. These campaigns achieve measurable systemic effects through:

- **Temporal Coordination**: Attacks consistently coincide with significant political events, military aid announcements, or sanctions implementation, demonstrating deliberate strategic timing
- **Resource Diversion**: Forcing disproportionate defensive expenditure relative to attack costs, creating asymmetric economic pressure
- **Psychological Operations**: Generating institutional uncertainty and eroding public confidence in digital service reliability
- **Geopolitical Signaling**: Demonstrating cyber capabilities while maintaining plausible deniability through civilian volunteer networks

The imperative to quantify and contextualize these multifaceted impacts has become critical for national security planning and resource allocation.

2. A Comprehensive Dual-Lens Cost Assessment Framework

To accurately evaluate how DDoSIA-driven campaigns affect national interests, we propose an integrated assessment model that:

- Calculates direct monetary costs through measurable economic impacts and response expenditures
- Employs a structured impact matrix to systematically evaluate broader strategic, social, and political consequences

This methodology ensures comprehensive coverage of both immediate financial burdens and long-term systemic vulnerabilities that traditional cost-benefit analyses typically overlook.

2.1 Quantitative Cost Model (Direct Economic Impact)

Formula: Total Quantitative Cost = $\Sigma[(Vi \times Di) \times Mi] + R + S$

Variable Definitions[2]**:**

[2] Mitigation Cost Estimates: The mitigation cost range in this model ($0.02–$0.15 per GB) reflects industry-informed approximations from DDoS protection providers such as Cloudflare, AWS Shield, and Akamai. These values estimate the cost of absorbing and filtering malicious traffic based on infrastructure type and operational complexity, forming the Mi component in the formula.

Actual mitigation costs vary depending on attack volume, duration, and response strategy. While these figures are not definitive, they serve as reasonable proxies for modeling direct costs. For greater

- **Core Attack Metrics:**
  - Vi = Volume of attack traffic (GB/second) for attack instance i
  - Di = Duration of attack i (hours)
  - Mi = Mitigation cost per GB of attack traffic (estimated $0.02-$0.15/GB based on infrastructure type)
- **Aggregate Response Costs (R):**
  - Emergency cybersecurity team deployment
  - Infrastructure hardening and repair
  - Opportunity cost of service disruption (deadweight loss from reduced economic activity)
  - Inter-agency coordination overhead
- **Sector-Specific Costs (S):**
  - Government services: Lost productivity, delayed public services (public sector multiplier effects)
  - Financial sector: Transaction processing delays, customer compensation (liquidity constraints and payment system friction)
  - Critical infrastructure: Service restoration, backup system activation (network externalities and cascading effects)
- **Macroeconomic Interpretation:**
  - **Multiplier Effects:** The R and S components (Aggregate Response Costs and Sector-Specific Costs) account for how initial cyber attacks create ripple effects throughout the economy, similar to how fiscal shocks propagate through interconnected markets.
  - **Deadweight Loss:** Service disruptions create economic inefficiencies where productive capacity is temporarily removed from the economy, generating welfare losses that exceed the immediate technical costs.
  - **Network Externalities:** Attacks on critical infrastructure (captured in S) create negative externalities where the social cost exceeds the private cost, as downstream users and connected systems experience cascading disruptions.
  - **Opportunity Cost:** The R variable includes foregone economic activity - resources diverted from productive uses to cyber defense represent a classic opportunity cost calculation.
  - **Market Failure Correction**: Government response costs (R) can be viewed as necessary public goods provision to address market failures in cybersecurity, where private actors under-invest in collective defense.

- **Application Example:** A coordinated 8-hour attack against Ukrainian government infrastructure averaging 1.5 GB/s with $0.08/GB mitigation costs yields $3,456 in

accuracy, analysts should calibrate using localized data, vendor contracts, or national CSIRT benchmarks.

immediate technical costs, before accounting for R and S multipliers, which our analysis suggests can increase total costs by 300-500%[3].

2.2. Qualitative Impact Matrix: Assessing Strategic and Social Consequences

Beyond financial costs, DDoS campaigns generate strategic impacts that affect national security, democratic processes, and international standing. Our framework evaluates these through four dimensions:

Impact Assessment Variables:

Dimension	Description	Assessment Scale	Key Indicators
Si	**Sector Criticality**	0-4 scale	Government (4), Financial (3), Infrastructure (3), Private (1-2)
Pi	**Public Disruption Factor**	0-5 scale	Media coverage intensity, service visibility, citizen complaints
G	**Geopolitical Impact**	0-5 scale	Diplomatic tensions, alliance strain, deterrence degradation
L	**Long-term Systemic Effects**	0-5 scale	Investment confidence, insurance premiums, innovation slowdown

2.3. Contextual Assessment Framework

2.3.1 High-Impact Scenarios (Based on our analysis):

- Attacks on electoral systems during voting periods (P=5, G=4-5)
- Sustained campaigns against financial infrastructure (S=3, L=3-4)

[3] This estimation of 300–500% in additional societal cost beyond immediate mitigation expenses is supported by sectoral analyses and cost modeling studies. For instance, the ENISA 2022 Threat Landscape report highlights that secondary impacts such as public service delays, reputational harm, and cross-sectoral disruptions frequently multiply initial technical costs several times, particularly in scenarios involving critical infrastructure. Likewise, data from the IBM Cost of a Data Breach Report 2024 and CISA's Cost of a Cyber Incident: Systematic Review and Cross-Validation suggest that national-level coordination, prolonged outages, and policy-level responses often drive aggregate cost increases well above baseline mitigation.

- Coordinated strikes during international crisis moments (G=4-5, P=3-5)

2.3.2 Moderate-Impact Scenarios:

- Routine government website disruptions (S=2-3, P=1-2)
- Brief attacks on commercial services (S=1-2, L=1-2)

This matrix enables policymakers to evaluate attacks beyond immediate technical metrics, incorporating strategic consequences that may exceed direct costs by orders of magnitude.

2.3.3 National Implementation and Societal Integration

Government Assessment Protocol: National governments can use this cost estimation model to generate comprehensive dual outputs to address significant cyber campaigns affecting their territories:

1. **National Cost Assessment**: Total societal impact calculated through the economic formula, aggregated across all affected sectors and regions
2. **Strategic Impact Evaluation**: National security consequence assessment using the multi-dimension matrix to inform policy responses

2.4 Government Decision-Making Applications:

By distinguishing between quantitative and qualitative impacts, this model equips governments with a dual-lens tool for rational decision-making. Each application area below translates cyber threat costs into actionable national policy levers.

2.4.1 National Resource Allocation

Governments can prioritize funding and infrastructure investment using quantifiable cyber costs and sectoral impact metrics. This ensures resources are directed to areas with the greatest societal return on protection.

- Federal budget prioritization for cybersecurity initiatives based on combined quantitative and qualitative threat scores
- Strategic defense investment allocation guided by sector-specific impact multipliers identified in threat assessments
- Emergency response funding calibrated to R-variable historical patterns

2.4.2 National Security Planning:

The model informs long-range planning by identifying where societal vulnerabilities accumulate and persist. Strategic foresight becomes more data-driven and responsive to evolving geopolitical cyber risk.

- Long-term national resilience investment strategies informed by L-variable trend analysis across multiple campaign cycles
- International alliance cooperation priorities determined through G-variable assessments of diplomatic and strategic costs
- Critical infrastructure protection policies based on sectoral impact data

2.4.3 Public Policy Communication:

Translating cyberattacks into both monetary and societal language strengthens public understanding and legislative alignment. This fosters trust, resilience, and political momentum for security initiatives.

- Transparent public reporting that contextualizes both direct economic costs and broader implications for national security
- Citizen education initiatives addressing societal digital resilience and individual preparedness responsibilities
- Legislative justification for cybersecurity appropriations using comprehensive cost-benefit analysis

2.5 Societal Integration Mechanisms:

The model promotes whole-of-society engagement by clarifying how cyber risk cascades across sectors. It encourages coordinated standards, partnerships, and long-term preparedness.

Cross-Sector Coordination:

- Public-private partnerships informed by shared understanding of true societal costs
- Industry-specific resilience standards based on sectoral impact multiplier data
- Academic and research institution collaboration on long-term strategic analysis

2.6 Integration with National Governance Frameworks:

This dual-lens model can be integrated with existing national security assessment methodologies while providing specific evaluation criteria for government decision-making. This enables seamless incorporation into:

- National security strategy development processes
- Congressional/Parliamentary budget oversight and appropriation decisions
- Inter-agency coordination mechanisms for crisis response
- International diplomatic engagement and treaty negotiation positions

This approach transforms cyber threat assessment from a technical exercise into a comprehensive tool for national governance and societal resilience planning.

3. Implications for National Cybersecurity Strategies

NoName057's DDoSIA operations demonstrate how distributed, ideologically-motivated cyber campaigns can achieve strategic effects through cumulative disruption rather than singular high-impact events. Our analysis of over 300,000 attacks reveals patterns of systematic targeting that align with broader geopolitical objectives while maintaining operational deniability.

The dual-lens cost assessment model addresses a gap in current cyber threat evaluation by recognizing that digital coercion operates simultaneously across economic and strategic dimensions. Traditional metrics focusing solely on bandwidth consumption or service downtime fundamentally underestimate the true impact of coordinated campaigns designed to erode institutional confidence and democratic stability.

3.1 Strategic Recommendations:

To counter the evolving complexity of ideologically motivated cyber campaigns, stakeholders must adopt a multidimensional approach. These recommendations align with the model’s dual focus on measurable economic damage and harder-to-quantify societal and strategic effects.

3.1.1 For Government Leaders:

Governments need structured, adaptive frameworks to assess and respond to cyber operations that target not only infrastructure but national stability. These recommendations emphasize systemic coordination and calibrated preparedness.

- Adopt comprehensive cost assessment frameworks that account for both direct and strategic impacts
- Develop sector-specific response protocols calibrated to impact multipliers identified in our analysis
- Establish inter-agency coordination mechanisms that can rapidly assess and respond to qualitative impact dimensions

3.1.2 For Cybersecurity Professionals:

Practitioners must evolve beyond purely technical playbooks and integrate threat context into operational workflows. These recommendations aim to strengthen both situational awareness and cross-domain response agility.

- Implement monitoring systems that capture both technical metrics and broader contextual indicators
- Develop response capabilities that address psychological and strategic dimensions of attacks, not merely technical disruption
- Engage in proactive threat intelligence sharing to identify campaign patterns and strategic timing

3.1.3 For Policy Makers:

Policy responses must reflect the hybrid nature of modern threat landscapes, balancing legal innovation with global cooperation. These actions help build national resilience and secure strategic advantage.

- Update legal frameworks to address the hybrid nature of ideologically motivated cyber operations
- Establish international cooperation mechanisms specifically designed for coordinated response to distributed campaigns
- Invest in national digital resilience programs that strengthen both technical defenses and societal preparedness

Conclusion

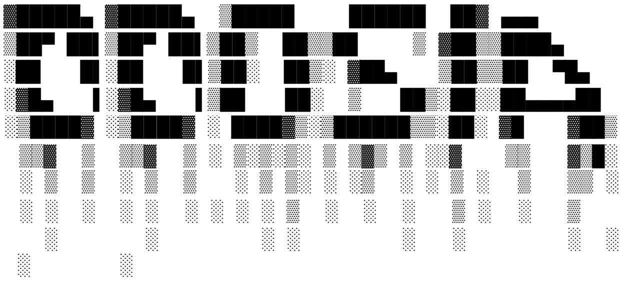
The evolution of cyber conflict toward distributed, ideologically motivated campaigns like those orchestrated by NoName057 requires fundamentally new approaches to impact assessment and strategic response. Traditional cybersecurity metrics, while necessary, are insufficient for evaluating threats that operate across multiple domains simultaneously.

Our dual-lens cost estimation model provides a framework for comprehensively assessing both the immediate economic burden and the broader strategic consequences of coordinated DDoS campaigns. By integrating quantitative financial analysis with systematic evaluation of strategic impacts, decision-makers can develop more effective defense strategies and resource allocation priorities.

This represents more than an evolution in cyber defense methodology, as it constitutes a recognition that digital conflict has become inseparable from broader questions of national resilience, democratic stability, and international security. The ability to accurately assess and respond to these multidimensional threats will increasingly determine national competitive advantage in an era of persistent digital confrontation.

As cyber operations continue to evolve in sophistication and strategic integration, the frameworks we develop today for understanding their true societal cost will shape our capacity to maintain democratic governance and social stability in an increasingly contested digital domain.

Annex: DDoSIA Campaign Analysis Data



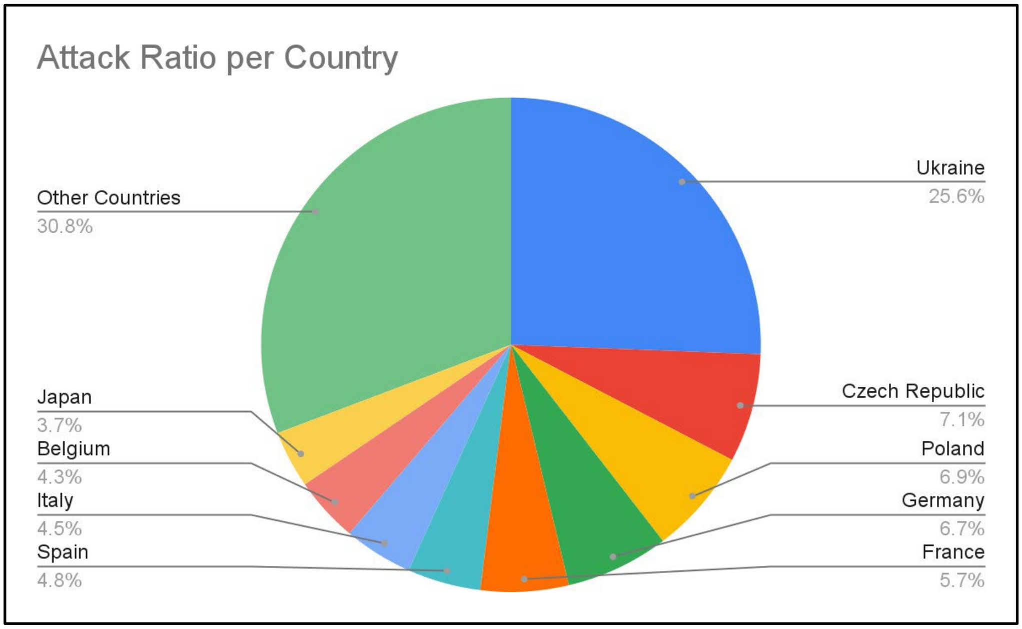
© Silas Cutler 2025

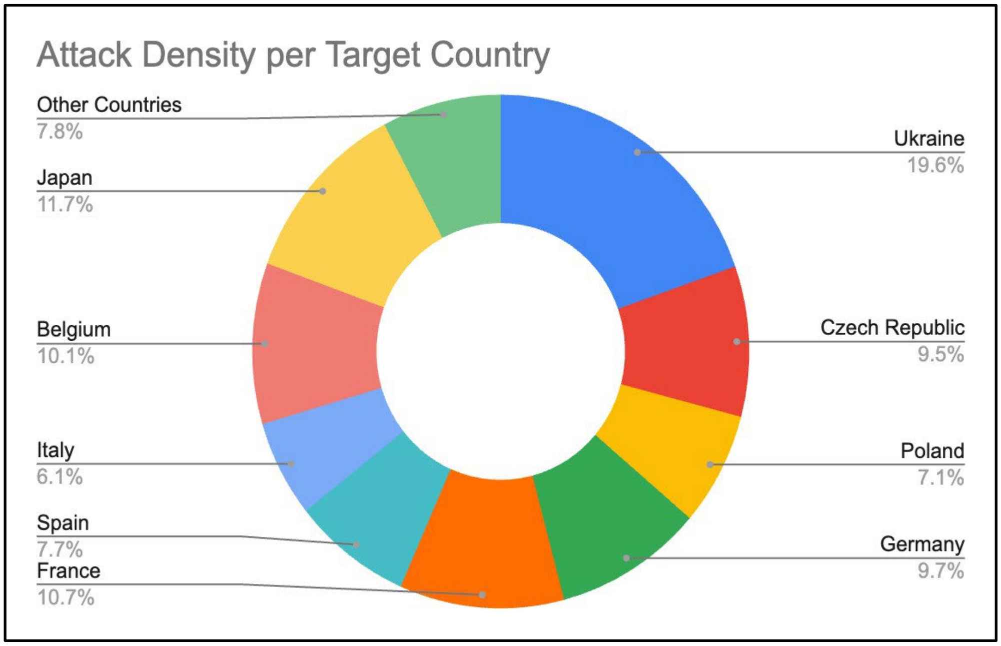
Dataset Overview

Dataset Overview	Summary
Total Records Analyzed: 304,659	**Total cyber attacks recorded:** 304,659
Date Range: February 8, 2023 to July 14, 2025	**Countries targeted:** 29
Analysis Period: 886 days	**Unique targets:** 5,895
	Government domains attacked: 59,505
	Campaign duration: 886 days

Top Targeted Countries

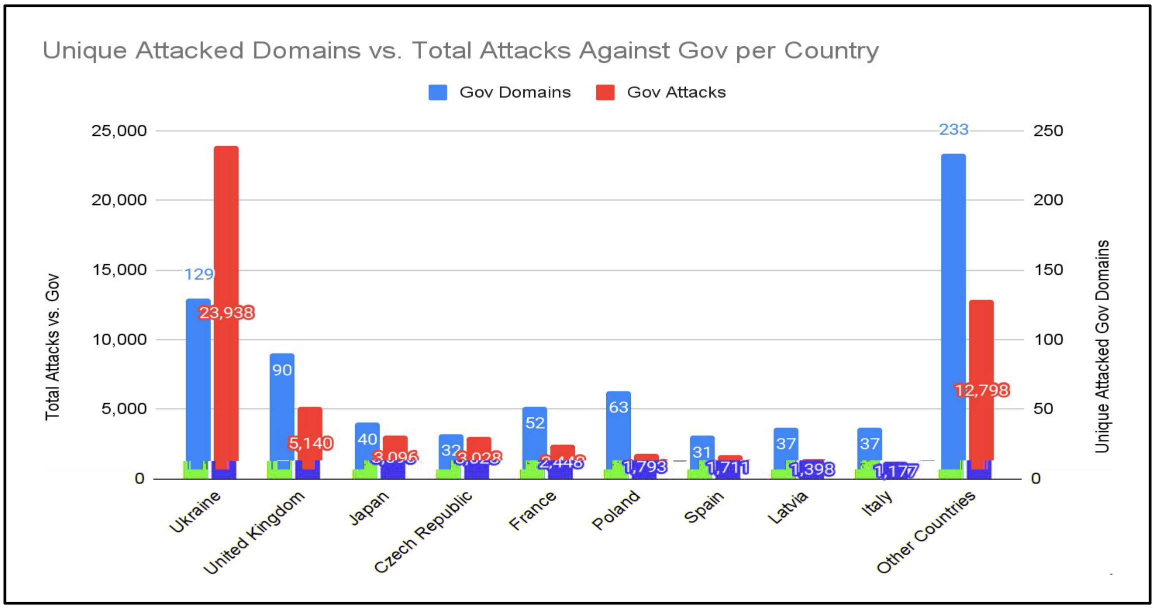
Rank	Country	Attacks	Unique Targets	Attack Density
1	Ukraine	63,749	525	121.4 attacks/target
2	Czech Republic	17,686	302	58.6 attacks/target
3	Poland	17,135	388	44.2 attacks/target
4	Germany	16,644	279	59.7 attacks/target
5	France	14,159	214	66.2 attacks/target
6	Spain	11,828	247	47.9 attacks/target
7	Italy	11,134	295	37.7 attacks/target
8	Belgium	10,589	169	62.7 attacks/target
9	Japan	9,320	129	72.2 attacks/target
10	Other Countries	76,727	1,599	48.0 attacks/target


Attack Ratio per Country
Ukraine
25.6%
Other Countries
30.8%
Czech Republic
7.1%
Poland
6.9%
Germany
6.7%
France
5.7%
Japan
3.7%
Belgium
4.3%
Italy
4.5%
Spain
4.8%


Attack Density per Target Country
Other Countries
7.8%
Ukraine
19.6%
Japan
11.7%
Belgium
10.1%
Czech Republic
9.5%
Italy
6.1%
Poland
7.1%
Spain
7.7%
Germany
9.7%
France
10.7%

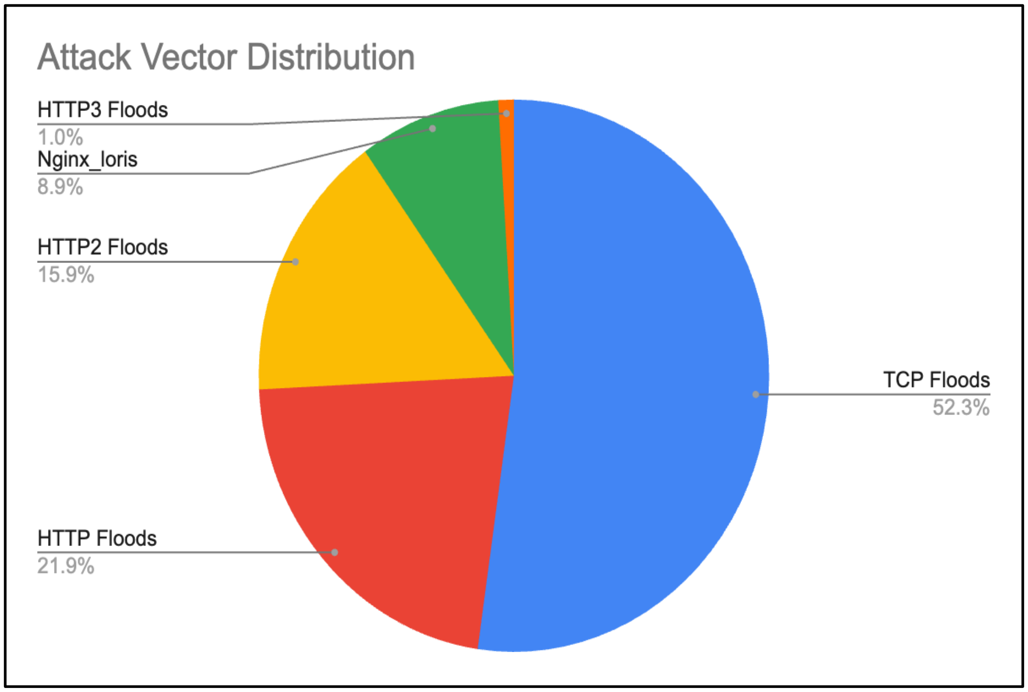
Government Infrastructure Targeting Analysis

Country	Gov Attacks	Gov Domains	Avg Attacks/Domain
Ukraine	23,938	129	185.6
United Kingdom	5,140	90	57.1
Japan	3,096	40	77.4
Czech Republic	3,028	32	94.6
France	2,448	52	47.1
Poland	1,793	63	28.5
Spain	1,711	31	55.2
Latvia	1,398	37	37.8
Italy	1,177	37	31.8
Other Countries	12,798	233	54.9



Attack Vector Distribution

Attack Type	Count	Percentage	Tactical Analysis
TCP Floods	157,997	51.90%	Volumetric overwhelm strategy
HTTP Floods	66,315	21.80%	Application-layer targeting
HTTP2 Floods	47,998	15.80%	Modern protocol exploitation
Nginx_loris	26,993	8.90%	Slow-connection attacks
HTTP3 Floods	2,978	1.00%	Protocol testing
Total	**302,281**	**99.40%**	*Remaining 0.6% distributed across other vectors*



Most Targeted Ukrainian Government Domains

Domain	Attacks	Strategic Significance
zp.gov[.]ua	946	Regional administration (Zaporizhzhia)
www.rada.gov[.]ua	841	National Parliament
rada-poltava.gov[.]ua	807	Regional Parliament (Poltava)
loga.gov[.]ua	698	Government logistics
smr.gov[.]ua	675	Municipal services
komfinbank.rada.gov[.]ua	672	Parliamentary financial committee
kompravpol.rada.gov[.]ua	672	Parliamentary legal affairs committee
komsamovr.rada.gov[.]ua	648	Parliamentary self-governance committee
kompravlud.rada.gov[.]ua	648	Parliamentary human rights committee
komzakonpr.rada.gov[.]ua	648	Parliamentary legislative committee
www.vmr.gov[.]ua	600	Municipal administration
mariupolrada.gov[.]ua	570	Mariupol city administration
komtrans.rada.gov[.]ua	560	Parliamentary transport committee
data.gov[.]ua	540	Open data portal
kompek.rada.gov[.]ua	528	Parliamentary economic committee

Sectoral Impact Analysis

Government & Public Administration: 59,505 attacks (19.5% of total)

- Focus on legislative, executive, and municipal institutions
- Particular emphasis on Ukrainian parliamentary infrastructure
- Secondary targeting of Western European government services

Critical Infrastructure: Estimated 45,000-50,000 attacks (14.7-16.4%)

- Financial services, transportation networks, utilities
- Cross-border coordination suggesting strategic planning

Private Sector: Remaining targets distributed across commercial entities

- Media organizations, educational institutions, private companies
- Often targeted in conjunction with government services

Temporal Analysis Highlights

- **Peak Activity Periods:** Attacks consistently intensified during:
    - Major military aid announcements to Ukraine
    - NATO summit periods
    - EU sanctions implementation phases
    - Ukrainian national holidays and commemorative dates
- **Campaign Coordination:** Evidence of centralized planning with distributed execution through volunteer networks

Geopolitical Targeting Pattern

The data reveals systematic targeting aligned with geopolitical positioning:

- **Primary Targets:** Ukraine and strong Ukrainian allies
- **Secondary Targets:** NATO/EU members providing military/financial support
- **Tertiary Targets:** Countries with significant diplomatic ties to Ukraine