When Code Hits Cold Metal: How Cybersecurity Manifests in the Physical World.

Vladimir Tsakanyan, Ph.D. · Center for Cyber Diplomacy and International Security

October 13, 2026

From sabotaged refrigeration systems in France to drone strikes on Russian data centers and AI-generated influence operations, October 2026 exposes a defining transformation in international security: digital infrastructure is no longer merely supporting the physical world. It is becoming inseparable from it.

Vladimir Tsakanyan, Ph.D. Center for Cyber Diplomacy and International Security (CCD-IS)

The End of the Virtual Battlefield

For much of the digital age, cybersecurity was understood primarily as the protection of information.

Governments defended networks. Companies protected databases. Security professionals investigated malware, patched software vulnerabilities and attempted to prevent unauthorized access.

The consequences of failure were often measured in stolen information, interrupted services or financial losses.

That distinction between the digital and physical worlds is increasingly difficult to maintain.

In October 2026, three seemingly unrelated developments illustrated the changing nature of technological vulnerability.

In France, attackers reportedly manipulated refrigeration-control systems at hundreds of supermarkets, disrupting temperature regulation and forcing businesses to discard food.

In Russia, Ukrainian drone strikes damaged data centers operated by Yandex, interrupting digital services and exposing the physical concentration of computing infrastructure.

Meanwhile, OpenAI disclosed an Iran-origin influence operation in which generative artificial intelligence was used to produce articles under deceptive author identities, allowing manipulated content to enter established information channels.

These incidents involved different actors, mechanisms and legal circumstances.

One was a cyber intrusion affecting industrial equipment.

Another involved physical military force directed against computing infrastructure.

The third concerned the manipulation of public information.

Yet together, they reveal a broader transformation.

Modern societies increasingly depend on systems in which software, physical infrastructure and human decision-making operate as a single interconnected environment.

The vulnerability of one layer can produce consequences throughout the others.

Cybersecurity has become a question of physical resilience, economic continuity and political stability.

1. France: When Software Controls the Food Supply

The French supermarket incident demonstrates the most direct relationship between digital compromise and physical consequences.

During the night of October 11–12, attackers reportedly exploited weaknesses in refrigeration-control systems used by multiple supermarket chains.

The affected retailers included Intermarché and Coopérative U, with additional disruptions reported at other French supermarket brands.

Investigations focused on older refrigeration-control technology associated with Danish manufacturer Danfoss.

The attackers reportedly manipulated operational settings, including defrosting functions, causing refrigerated and frozen storage units to lose their required temperature conditions.

The consequences were immediate.

Food products became unsafe or unsuitable for sale.

Businesses were forced to discard inventory.

Store operations were disrupted.

French authorities opened a cybercrime investigation.

This was not simply an attack on information.

It was an attack on a physical process controlled through information technology.

The difference is fundamental.

A conventional data breach may expose customer records.

A compromised refrigeration controller can destroy food.

The attacker does not need to enter the building, damage a compressor or physically disconnect electrical equipment.

The malicious action can occur remotely, while the resulting damage appears inside a supermarket.

Software becomes an instrument for manipulating matter.

2. The Historical Development of Cyber-Physical Vulnerability

The relationship between computers and industrial machinery is not new.

Industrial control systems have operated essential infrastructure for decades.

Supervisory Control and Data Acquisition systems, programmable logic controllers and specialized industrial networks have long regulated electricity, manufacturing, transportation and water systems.

Historically, many of these environments were relatively isolated from public networks.

Security relied partly on physical separation.

Over time, economic and operational incentives encouraged greater connectivity.

Remote maintenance reduced costs.

Centralized monitoring improved efficiency.

Cloud platforms enabled real-time analysis.

Industrial Internet of Things devices expanded the number of connected sensors and controllers.

But connectivity also created new paths for intrusion.

Equipment designed for operational reliability rather than hostile network environments became accessible through increasingly complex digital systems.

The resulting vulnerability is structural.

An industrial controller may remain functional for many years after its software is no longer actively maintained.

Replacing it can be expensive.

Taking it offline can interrupt essential operations.

Organizations therefore face pressure to continue using systems whose cybersecurity protections are outdated.

The French refrigeration incident illustrates the consequences of this technological inheritance.

The problem is not simply that attackers discovered a vulnerability.

It is that physical infrastructure can remain dependent on obsolete software long after the security environment has changed.

3. From Stuxnet to the Supermarket

The modern history of cyber-physical operations provides important context.

In 2010, the discovery of Stuxnet demonstrated that malicious software could manipulate industrial processes with destructive physical consequences.

The operation targeted Iranian nuclear enrichment equipment, altering centrifuge behavior while attempting to conceal the manipulation.

Stuxnet became a landmark because it challenged the assumption that cyber operations were primarily concerned with information.

Software could produce mechanical damage.

In December 2015, a cyberattack disrupted electricity distribution in Ukraine, demonstrating that attackers could remotely interfere with power-grid operations.

A subsequent attack in 2016 further highlighted the vulnerability of industrial electrical systems.

In 2017, the Triton malware targeted a safety-instrumented system at an industrial facility in Saudi Arabia.

That case was particularly significant because safety systems exist to prevent dangerous industrial conditions.

Compromising them can potentially undermine the mechanisms designed to protect human life.

In 2021, the Colonial Pipeline ransomware incident in the United States demonstrated a different relationship between cyber and physical disruption.

The attack affected business IT systems, prompting the company to shut down pipeline operations as a precaution.

The resulting fuel-distribution disruption illustrated how a cyber incident can affect physical supply chains even without directly manipulating industrial equipment.

The French supermarket incident belongs within this historical progression.

Its importance is not that refrigeration systems are strategically equivalent to nuclear facilities or national power grids.

They are not.

Its importance is that cyber-physical vulnerability has extended into ordinary commercial environments.

A supermarket refrigeration controller can now become the endpoint of a remote cyberattack.

The consequences reach consumers, employees, food suppliers and local communities.

Cyber-physical risk is no longer confined to facilities traditionally classified as national-security infrastructure.

4. Food Security as a Cybersecurity Problem

Food security is generally discussed in terms of agricultural production, climate conditions, transportation, trade and prices.

Cybersecurity adds another dimension.

Modern food systems depend on refrigeration, warehouse automation, logistics software, digital payment systems and coordinated distribution networks.

Cold-chain infrastructure is particularly sensitive.

Perishable goods require controlled temperature conditions during storage and transportation.

Disrupting those conditions can destroy inventory even when production and transportation remain otherwise functional.

This creates an asymmetry.

An attacker may need access to only a limited number of digital control systems to generate substantial physical and economic losses.

The cost of intrusion can be far lower than the cost of recovery.

That asymmetry makes ordinary commercial infrastructure strategically relevant.

A coordinated attack on food storage and distribution could create shortages, financial pressure and public anxiety.

The French incident does not establish that such a broader campaign occurred.

But it demonstrates a mechanism through which digital compromise can affect the physical availability of essential goods.

The political implication is significant.

Governments may increasingly need to treat certain commercial cyber-physical systems as components of national resilience, even when they are privately owned and not traditionally classified as critical infrastructure.

5. Russia: When Physical Force Disrupts the Cloud

The Yandex data-center attacks demonstrate the reverse relationship.

Instead of using software to manipulate physical equipment, military force was used against the physical infrastructure supporting digital services.

On October 8 and 9, Ukrainian drone attacks damaged Yandex facilities in Sasovo and Kaluga.

Yandex confirmed that the Sasovo facility was shut down and that part of the Kaluga infrastructure was out of service.

The company acknowledged disruptions affecting customers and businesses dependent on its services.

Reuters reported difficulties involving several Russian online platforms and described the challenge of transferring affected workloads to alternative cloud providers.

The full extent of the outages and any permanent data losses remained uncertain.

Nevertheless, the strategic implication was clear.

Cloud infrastructure is physical infrastructure.

Its services may be accessed through intangible digital interfaces, but its operations depend on buildings, electrical systems, cooling equipment, fiber-optic connections and computing hardware.

Destroy or disable those components and digital capability can disappear.

The cloud is not outside geography.

It is concentrated within it.

6. The Strategic Geography of Computing

The digital economy has encouraged the concentration of computing capacity.

Large data centers benefit from economies of scale.

They can share electricity, cooling systems, network connections, physical security and specialized maintenance.

Artificial intelligence has reinforced this trend.

Training advanced models requires large quantities of computing power.

The necessary hardware is expensive and energy-intensive.

Concentrating computing infrastructure can improve efficiency.

But concentration also creates vulnerability.

A limited number of facilities may support a disproportionate share of national digital activity.

A single damaged facility can affect many organizations that do not own or operate the underlying infrastructure.

This creates a strategic dependency that is often poorly understood outside the technology sector.

A business may believe it operates independently because it has its own website, customer database and application.

In practice, those services may depend on the same cloud provider as thousands of other businesses.

The failure of one physical location can therefore produce simultaneous disruptions across otherwise unrelated sectors.

The Yandex attacks illustrate how a physical strike against a technology provider can create downstream economic and operational effects.

They also demonstrate why geographic redundancy is becoming a national-security concern.

7. Data Centers as Strategic Infrastructure

Historically, military planners focused on infrastructure whose strategic significance was immediately visible.

Railways moved troops.

Ports supported trade and naval operations.

Bridges enabled transportation.

Power plants supplied electricity.

Telecommunications facilities enabled command and coordination.

Data centers now perform functions that are similarly important to modern societies.

They support financial services, transportation applications, government platforms, communications, logistics and artificial intelligence.

Their importance extends beyond commercial convenience.

Advanced computing infrastructure can also support military research, intelligence analysis and defense-related technology.

This creates a difficult problem during armed conflict.

Some computing facilities may have exclusively civilian functions.

Others may support both civilian and military activities.

International humanitarian law does not treat all economically or technologically important infrastructure as a lawful military target.

The legality of an attack depends on the circumstances, including whether the object qualifies as a military objective and whether the applicable rules of distinction, proportionality and precautions are respected.

A data center's general importance to an adversary's economy is not, by itself, sufficient to establish that it may lawfully be attacked.

The emerging strategic importance of data centers therefore creates both operational opportunities and legal complications.

8. The AI Compute Problem

The Yandex case also raises questions about artificial intelligence infrastructure.

Yandex previously identified its Sasovo facility as housing major computing resources used in the development of its AI systems.

Reuters reported that two of the company's three supercomputers used for model development were located at that site, although their condition after the strike was not established.

This matters because advanced AI development depends on concentrated computational resources.

For decades, the principal strategic assets of the digital economy were often described as software, algorithms and data.

The rise of computationally intensive AI has renewed the importance of physical industrial capacity.

Semiconductors must be manufactured.

Servers must be assembled.

Electricity must be supplied.

Cooling systems must operate.

Data centers must be protected.

AI capability therefore depends on a physical supply chain that can be disrupted through conventional means.

This is a notable historical reversal.

The digital revolution was frequently described as reducing the importance of geography.

The AI revolution is making geography strategically important again.

9. The Convergence of Kinetic and Cyber Operations

The relationship between physical force and digital capability is becoming increasingly reciprocal.

Cyber operations can interfere with physical systems.

Physical attacks can disable digital infrastructure.

The two methods can also reinforce one another.

A cyber operation might disrupt communications before a physical attack.

A physical strike might destroy the computing infrastructure needed for cyber defense.

An attack against electricity infrastructure can interrupt digital services without compromising a single computer.

A cyberattack against industrial controls can produce physical damage without using explosives.

These possibilities create new operational combinations.

But they should not be collapsed into one category.

A drone strike against a data center remains a physical attack, even when its consequences are digital.

A remote intrusion into an industrial controller remains a cyber operation, even when its consequences are physical.

The distinction matters for attribution, legal analysis and military doctrine.

The broader phenomenon is best understood as the convergence of cyber and physical security rather than the disappearance of their differences.

10. Information Operations: A Third Path to Physical Consequences

The third development concerns a different form of vulnerability.

On October 8, OpenAI disclosed an Iran-origin operation using its models to produce articles and editorial material under deceptive author identities.

The operation used several fictitious bylines and attempted to place content in established publications.

OpenAI identified nearly 100 published or syndicated articles across more than a dozen outlets.

The Washington Post subsequently reported that the activity had reached at least 20 publications.

The articles focused heavily on the U.S.–Iran conflict and related political issues.

OpenAI said the activity appeared consistent with a commercial influence operation, but it did not establish the identity of the ultimate operator.

This distinction is essential.

The evidence supports describing an Iran-origin deceptive influence operation.

It does not establish that the Iranian government directed the campaign.

The incident nevertheless demonstrates an important vulnerability in modern information systems.

Artificial intelligence can make it easier to manufacture the appearance of legitimate human authorship.

11. The Industrialization of Credibility

Information manipulation is not new.

Governments and political organizations have used propaganda, forged documents, covert publications and deceptive identities for centuries.

During the Cold War, influence operations sometimes relied on fabricated stories distributed through sympathetic or unwitting intermediaries.

The objective was not always to convince audiences directly.

It was often to place a claim inside a seemingly credible institution, allowing that institution's reputation to amplify the message.

Generative AI reduces the cost of producing such material.

An operator can generate articles, revise their tone, adapt them to editorial requirements and create multiple author identities.

The resulting content may enter publications through ordinary submission processes.

The vulnerability is therefore not simply technological.

It is institutional.

Editorial systems depend on assumptions about authorship, provenance and good-faith participation.

AI-generated deceptive content exploits those assumptions.

The political significance lies in the laundering of credibility.

A fabricated author may be unknown.

But once that author's article appears in a recognized publication, readers may interpret the material through the reputation of the outlet.

That is how synthetic information can acquire real-world influence.

12. From Information Manipulation to Political Behavior

The relationship between information operations and physical consequences is less direct than in industrial sabotage.

A compromised refrigeration controller can immediately alter temperature.

A destroyed data center can immediately interrupt computing capacity.

An influence campaign operates through human interpretation.

It may seek to affect public attitudes, political debate, voting behavior, diplomatic perceptions or institutional trust.

Those outcomes are difficult to measure.

Publication alone does not establish persuasion.

Exposure does not prove behavioral change.

And an influence operation's intended effects should not be confused with demonstrated results.

Nevertheless, information integrity is an important component of national security.

Governments make decisions based on information.

Citizens evaluate public policy through information.

Financial markets respond to information.

Diplomatic relationships can be affected by information.

The manipulation of trusted information channels can therefore have consequences beyond the digital environment.

The cyber-physical relationship is not limited to machines.

It also includes the institutions and decisions through which information shapes human activity.

13. Three Incidents, Three Different Legal Problems

The October incidents also illustrate why international security institutions face growing difficulties in classifying technologically mediated harm.

The French refrigeration attack raises questions of cybercrime, industrial cybersecurity, product security and potentially state responsibility if credible evidence of state involvement emerges.

The Yandex data-center strikes raise questions under the law of armed conflict, including the status of computing infrastructure and the protection of civilians.

The AI-generated influence campaign raises questions about deceptive political activity, media integrity, platform governance and possible foreign interference.

These are not legally identical.

Different rules apply.

Different standards of attribution apply.

Different authorities are responsible for investigation and response.

The challenge is that the consequences can converge.

Economic disruption.

Public uncertainty.

Institutional distrust.

Interruption of essential services.

Pressure on governments.

Modern hybrid conflict often exploits this convergence.

A state may experience several kinds of disruption simultaneously without being able to treat them as one legally unified attack.

14. The Problem of Civilian Infrastructure

One of the most consequential political developments is the growing strategic importance of civilian technology.

Private companies operate much of the infrastructure on which national economies depend.

Cloud providers support government services.

Telecommunications firms maintain communications networks.

Retailers manage food distribution.

Logistics companies coordinate supply chains.

Technology platforms shape public information environments.

This creates an unusual relationship between private ownership and public security.

The state may be responsible for protecting national resilience without directly controlling the systems on which that resilience depends.

Private operators, meanwhile, may be responsible for infrastructure whose disruption has consequences far beyond their own businesses.

Traditional divisions between corporate cybersecurity and national security become increasingly inadequate.

The solution is not necessarily greater state control over private infrastructure.

It is a more developed system of shared responsibility.

Governments need visibility into systemic dependencies.

Companies need realistic security obligations.

Regulators need to account for the physical consequences of digital failures.

And emergency planning must address dependencies across organizational boundaries.

15. The Political Economy of Digital Dependence

The convergence of digital and physical vulnerability is also a consequence of economic organization.

Modern technology systems prioritize efficiency.

Centralized infrastructure reduces costs.

Remote administration reduces maintenance requirements.

Shared platforms accelerate deployment.

Automation reduces labor demands.

Cloud computing allows businesses to operate without maintaining their own physical servers.

These developments have produced enormous economic benefits.

But efficiency and resilience are not identical.

A highly optimized system may contain limited spare capacity.

A centralized platform may create a single point of failure.

A remotely managed industrial system may expand its attack surface.

A supply chain dependent on continuous digital coordination may have little tolerance for interruption.

The political problem is that the economic benefits of concentration are often immediate, while the costs of systemic vulnerability become visible only during a crisis.

Governments therefore face a difficult regulatory challenge.

How much redundancy should essential infrastructure maintain?

Who should pay for it?

Should critical services be required to preserve offline operating capabilities?

Should obsolete industrial controllers be subject to mandatory replacement schedules?

Should cloud providers disclose geographic concentration risks?

These questions increasingly belong to economic and security policy simultaneously.

16. Digital Sovereignty Is Physical Sovereignty

The concept of digital sovereignty is often discussed in relation to data localization, foreign technology providers and government authority over digital systems.

The October incidents reveal a more concrete dimension.

A country may possess legal control over its data while remaining physically dependent on vulnerable infrastructure.

A domestic cloud provider may reduce certain foreign dependencies while concentrating national computing resources in a small number of facilities.

A government may regulate software security while overlooking the physical systems that software controls.

A society may possess advanced digital services without adequate mechanisms for operating essential functions during an outage.

Sovereignty therefore cannot be measured solely by ownership or jurisdiction.

It must also be measured by resilience.

Can essential services continue when networks fail?

Can industrial equipment operate safely without remote connectivity?

Can digital services recover after physical destruction?

Can institutions distinguish authentic information from coordinated deception?

These questions are becoming central to the practical meaning of technological independence.

17. Cyber Diplomacy Must Move Beyond Network Security

International cyber diplomacy has historically focused on responsible state behavior, international law, confidence-building measures and the prevention of conflict in cyberspace.

Those priorities remain necessary.

But cyber diplomacy must increasingly address the physical dependencies of digital societies.

This includes the protection of civilian cyber-physical infrastructure.

It includes cooperation on industrial-control-system security.

It includes the resilience of cloud infrastructure and telecommunications networks.

It includes incident notification when cross-border services are disrupted.

It includes mechanisms for investigating state-linked cyber operations.

And it includes the governance of AI-enabled influence campaigns.

The challenge is not simply establishing rules for what states may do online.

It is developing international expectations for protecting the physical systems on which digital life depends.

The United Nations framework on responsible state behavior in cyberspace already provides important foundations, including norms concerning critical infrastructure.

The next stage requires translating those principles into practical resilience.

18. The Limits of Deterrence

Traditional deterrence assumes that an adversary can be discouraged through the threat of consequences.

Cyber-physical vulnerabilities complicate this logic.

An attack may be difficult to attribute.

The attacker may operate through criminal intermediaries.

The damage may result from the manipulation of ordinary commercial technology.

A physical strike may produce digital consequences extending far beyond the intended target.

An influence operation may achieve partial effects without any single event that clearly justifies retaliation.

Governments therefore cannot rely exclusively on threatening punishment.

They must also reduce the benefits available to attackers.

This is the logic of deterrence by denial.

A refrigeration system with effective segmentation and safe local controls is harder to manipulate remotely.

A cloud platform distributed across geographically separated facilities is harder to disable through one physical strike.

An editorial organization with stronger author-verification procedures is harder to exploit through fabricated identities.

Resilience reduces the expected effectiveness of hostile operations.

In a highly interconnected society, that may be as important as retaliation.

19. Building Resilience Across Three Domains

The incidents point toward a security model integrating three areas that are often managed separately.

Operational resilience concerns the safe functioning of physical systems controlled by software.

It requires secure industrial controllers, supported firmware, network segmentation, monitoring and the ability to maintain safe operating conditions when digital connectivity fails.

Infrastructure resilience concerns the physical foundations of computing.

It requires geographic redundancy, backup power, diversified connectivity, tested recovery procedures and realistic assessments of concentrated infrastructure risk.

Information resilience concerns the integrity of institutions through which societies understand events.

It requires provenance verification, transparent editorial practices, investigative capacity and public awareness of deceptive information operations.

None of these measures is sufficient alone.

A society can possess strong network defenses while remaining vulnerable to physical destruction.

It can maintain redundant data centers while relying on insecure industrial controllers.

It can protect infrastructure while allowing its information environment to be manipulated.

Modern resilience requires all three.

20. The New Geography of National Security

The deeper historical change is the return of geography to digital security.

For years, the language of cyberspace encouraged the impression that digital systems operated beyond physical territory.

Cloud computing reinforced this abstraction.

Data appeared accessible from anywhere.

Services seemed independent of location.

Digital platforms appeared to exist as continuously available utilities.

But every digital service depends on physical systems.

Electricity.

Cooling.

Buildings.

Semiconductors.

Communications cables.

Industrial equipment.

Human operators.

Political institutions.

The October incidents expose different parts of that dependency.

France demonstrates that digital commands can change physical conditions.

Russia demonstrates that physical destruction can disable digital capability.

The influence operation demonstrates that synthetic information can enter real institutions and potentially affect political decision-making.

The digital world has never been separate from the physical world.

Its dependence has simply become more consequential.

Bottom Line Assessment

The defining cybersecurity challenge of the coming decade may not be the protection of information alone.

It may be the protection of the systems through which information controls physical processes, supports essential services and influences political decisions.

The French refrigeration attacks show how a software vulnerability can create immediate material losses.

The Yandex data-center strikes show how conventional military force can disrupt digital infrastructure and the economic activities dependent upon it.

The AI-generated influence campaign shows how synthetic content can exploit institutional trust and enter public debate under deceptive identities.

These incidents should not be treated as one coordinated campaign.

Nor do they establish that all cyber threats produce physical damage.

Their significance lies in the structural relationship they reveal.

Modern societies are increasingly organized around interconnected digital and physical systems.

Those systems generate efficiency, innovation and economic opportunity.

They also create dependencies that adversaries, criminals and other malicious actors may exploit.

For governments, the strategic priority must therefore expand from protecting networks to protecting continuity.

For companies, cybersecurity must become part of operational safety and business resilience.

For international institutions, cyber diplomacy must account for the physical consequences of digital disruption.

And for national-security policymakers, the distinction between digital infrastructure and strategic infrastructure is becoming increasingly artificial.

The cloud is made of steel, silicon, electricity and concrete.

Industrial systems obey software instructions.

Public institutions depend on the integrity of information.

The boundary between code and the physical world has not disappeared because technology has become intangible.

It has disappeared because technology now governs so much of what is tangible.

The next generation of cybersecurity strategy must protect not only the information society produces, but the physical society that information increasingly controls.

Vladimir Tsakanyan, Ph.D. Center for Cyber Diplomacy and International Security (CCD-IS)

Sources and links

[1] Vladimir Tsakanyan, Ph.D.

https://cybercenter.space/vladimir-tsakanyan/

Read the original article online

https://cybercenter.space/2026/10/13/when-code-hits-cold-metal-how-cybersecurity-manifests-in-the-physical-world/