

Civilian Digital Ecosystems at the Core: Safeguarding During Crisis



• **Orientation Note:** •

This report is intended for a broad range of stakeholders engaged in digital policy, resilience, and emergency preparedness. It serves as a practical reference to inform coordinated approaches and shared understanding.



Executive Summary

Crisis today does not stop at physical borders, it extends into the digital systems that power everyday life. Healthcare platforms, payment infrastructure, civil registries, emergency alert systems, and utilities are all increasingly dependent on digital networks. When those networks are disrupted, whether through cyber-incidents, physical destruction, or deliberate manipulation of information — the consequences for civilian populations can be severe and immediate.

International law already recognizes the importance of protecting civilian infrastructure. As those systems migrate online, that obligation extends to the digital realm. Yet implementation remains uneven across contexts and the use of “the dual-use nature of some digital systems” justifications continues to expose civilian digital systems to deliberate targeting. This report, prepared by the Digital Cooperation Organization (DCO) General Secretariat, identifies four categories of threats, ranging from AI-enabled disinformation to physical destruction of submarine cables and data centers, and proposes a coordinated response framework built around four strategic tracks:



Resilience

Strengthening the physical and technical robustness of civilian digital infrastructure, including Internet Exchange Points (IXPs), submarine cables, and essential service platforms.



Trust

Protecting official government communication channels and equipping the public with tools to recognize and respond to misleading information.



Knowledge Sharing

Establishing rapid coordination mechanisms and enabling governments to exchange expertise, threat intelligence, and technical solutions.



Service Continuity

Defining minimum standards for the restoration of essential digital services in a timely manner following disruption, with strong data governance safeguards.

The report highlights a set of priority actions for governments, including strengthening coordination, enhancing communication reliability, and assessing digital infrastructure resilience, supported by a phased approach to implementation.

The DCO stands ready to support stakeholders, including governments through its Digital Economy Navigator, AI governance tools, cross-border data frameworks, and multi-stakeholder network. Protecting civilian digital ecosystems is not only a humanitarian imperative, it is a prerequisite for effective governance, economic stability, and social cohesion in times of crisis.



A. Context and purpose

1 In situations of crisis, the disruption of civilian digital ecosystem (physical and non-physical) can severely affect the provision of essential services that civilians depend on daily. Critical services, such as Healthcare systems, financial platforms, social protection systems, utilities, and emergency response services increasingly rely on digital infrastructure. When this infrastructure is disrupted (due to military or cyber-related disruptions), civilians may lose access to vital public services at the moments they need them most.



2 In addition to the threats to digital services and infrastructure, recent conflicts have also been characterized by an increased negative use of digital tools and solutions in ways that may have direct or indirect impacts on civilian populations.

For instance, the manipulation of emergency information, the impersonation of official communication channels, or the rapid spread of unverified or AI-generated content can trigger social unrest, undermine public trust, and hinder emergency response efforts.

Even unintentionally, the sharing of sensitive information through social media, such as real-time images and locations of military operations, may expose civilians, emergency responders, or critical infrastructure, to increased risks.

3 International Humanitarian Law (IHL) has long established that civilian infrastructure should be protected (Geneva Conventions and their Additional Protocols) and objects indispensable to civilian survival, including water, power, and medical systems, enjoy explicit legal protection which means that deliberate attacks against them constitute war crimes.

These principles apply equally to the digital realm. As critical infrastructure migrates online, international law therefore requires that digital systems serving civilian populations receive equivalent protection. And yet, application remains inconsistent.

The most frequently invoked justification is the “dual-use doctrine” whereby governments and other actors may argue that civilian infrastructure simultaneously serves military purposes, thereby making it a legitimate target. Actors argue that civilian infrastructure simultaneously serves military purposes, thereby rendering it a legitimate target.

4 In order to address the challenges caused by an increased risk on civilian digital ecosystems alongside evolving and uneven legal frameworks there is need to strengthen efforts among relevant stakeholders to enhance resilience and sustainable development of the civilian digital ecosystems.

5 As an international intergovernmental organization mandated to enable digital prosperity for all and foster digital cooperation and resilience, the DCO works through its flagship initiatives to advance collaborative approaches that strengthen the security, resilience, and sustainability of digital ecosystems during crises.

B. Understanding the Threat landscape

6 To promote the effective design, planning, and implementation of measures aimed at strengthening the resilience and protection of civilian digital ecosystems in situations of instability or crisis, it is important to assess potential threats across two main dimensions:

The nature of the attack vector (digital or physical) and the primary effect (kinetic or non-kinetic). An analysis based on two (2) dimensions allows us to define four (4) categories which will help effects to structure assessment and coordinated actions among stakeholders, including governments.

Category 1: Digital threat with non-kinetic effects.



Targets include trust, perception, decision-making and societal and economic cohesion. In the digital era, this category is amplified and accelerated by the format and the scale provided by new tools (incl. Generative AI).

Examples:

- 01 Online Content mis- and dis-information
- 02 Cognitive warfare
- 03 Cyber-attack (soft) that disrupt digital activities (e.g. services, payments, etc.)

Category 2: Physical threat with non-kinetic effects.



This is related to traditional large-scale physical disruptions affecting infrastructure and access to essential resources. The effects accumulate through systemic disruption of social and economic activities.

This category traditionally includes disruptions to supply chains and critical services which indirectly impacts the digital ecosystem.

Examples:

- 01 Indirect disruption of e-government services.
- 02 Indirect erosion of the Innovation Driven Entreprises ecosystem in terms of operations, attractivity and expansion.

Category 3: Digital threat with kinetic effects.



In this category, despite the fact that the attack vector is virtual, the outcome is impacting the “real world” and can cause physical harm and disruption to civilian populations and infrastructure.

Examples:

- 01 Cyber-attack (hard) targeting of primary essential infrastructure (water and electricity).
- 02 Voluntary and involuntary weaponization of social media (incl. exploitation of open-source intelligence to identify civilian targets).
- 03 Cyber-attack redirecting the use of weapons against civilian areas and populations.

Category 4: Physical threat with kinetic effects.



This is the most conventional category of physical disruptions where, by default, non-digital attack vectors are causing physical destruction. However, in the digital ecosystem, these physical destructions can have direct effect on the continuation of digital activities.

Examples:

- 01 Destruction of physical infrastructure, incl. Data Centers, Submarine Cables, Mobile Network
- 02 Staff safety impact for Government, Private Sector, and Partners

PHYSICAL VECTOR

DIGITAL VECTOR

KINETIC EFFECT

Physical Threat Kinetic Effect

Conventional physical operations causing physical destruction with direct effects on the continuation of digital activities.

EXAMPLES

- Destruction of data centres
- Submarine cable damage
- Mobile network destruction
- Staff safety impact

Digital Threat Kinetic Effect

Virtual attack vectors with real-world physical outcomes, including potential civilian casualties.

EXAMPLES

- Cyber-attacks on water/electricity
- Cyber-redirected weapons
- Weaponisation of social media
- OSINT targeting civilians

NON-KINETIC EFFECT

Physical Threat Non-Kinetic Effect

Traditional coercive physical disruptions with systemic disruption of social and economic activities affecting digital ecosystems indirectly.

EXAMPLES

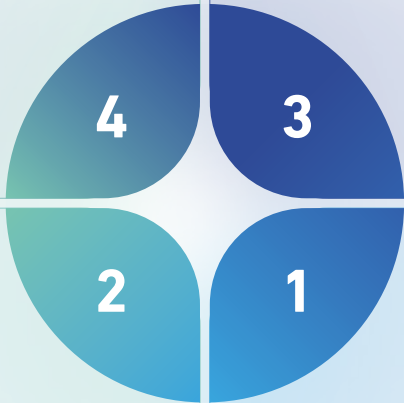
- Disruption of e-government
- Supply route blockades
- Erosion of innovation ecosystem

Digital Threat Non-Kinetic Effect

Targets trust, perception, decision-making and societal cohesion. Amplified and accelerated by GenAI tools at unprecedented scale and speed.

EXAMPLES

- Mis/disinformation
- Cognitive warfare
- Soft cyber-attacks on services



7 To contextualize the analysis and recommendations of this report, it is important to list the emerging threats that are either enabled/accelerated by digital solutions, or/and impacting directly the digital ecosystem supporting civilian activities (social, political, and economic).

These emerging trends have been identified based on observations from recent global developments and crisis situations.

I AI-Generated Misinformation and Disinformation

In the current crisis landscape we can observe large-scale manipulation of the information environment using Artificial Intelligence tools to fabricate content at unprecedented scale and speed, undermining the integrity and resilience of civilian digital ecosystems.

GenAI tools have dramatically lowered the barrier to producing convincing fabricated video content. What once required professional production capabilities can now be generated by a single individual within minutes.



This unprecedented speed makes factchecking nearly impossible: by the time a video is identified as false, it may have been viewed by millions of users, shaped public perception, and even triggered reactions.

AI-generated images, and synthetic content may be used to describe events that either did not occur or were materially misrepresented. Key drivers of this emerging use of GenAI in crisis context:

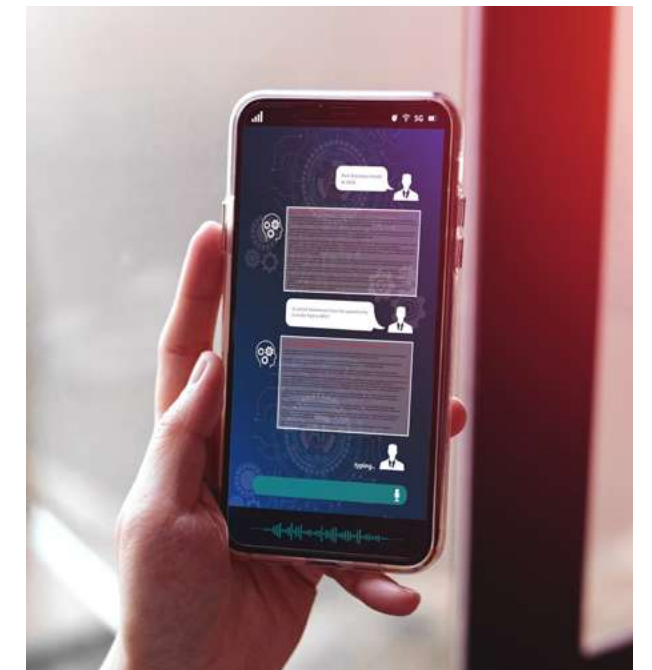
- 01 Actors distribute AI-generated conflict-related content
- 02 Opportunistic actors, including individuals, are sharing synthetic content, recycled footage from other contexts, or digitally altered media presented as real events, often amplified through online engagement dynamics.

The practical consequences for civilians are severe: populations cannot reliably distinguish genuine emergency alerts from fabrications; public trust in official government communications erodes; and the psychological burden of an already traumatic environment is compounded by deep uncertainty about what information can be trusted.

II Inadvertent Civilian Disclosure of Sensitive Information

Another digital-related emerging risk arose directly from civilian behavior: well-intentioned citizens are inadvertently sharing content that reveals operationally sensitive information in ways that place others at risk. We present the following evidence from the literature on crises and conflicts to illustrate this trend:

- 01 Publicly shared geotagged photographs and videos from conflict zones can reveal civilian locations, including civilian shelters, humanitarian convoys, medical facilities, and critical infrastructure, potentially exposing them to risk, allowing adversaries or automated systems to extract spatial intelligence in real time via AI and open source intelligence (OSINT) methods^[1].
- 02 Real-time posts on social media and digital platforms sharing conflict-related developments, within an environment where social media has transformed the speed, reach, and strategic role of information in crises warfare conflict, enable near real-time global dissemination, blurring the line between civilian communication and information operations broader information environments and increasing the risk that sensitive information may be exploited for misinformation campaigns^[2].



- 03 Sharing of unofficial or unverified information, such as rumors about crisis-related incident locations and casualty numbers, through diverse sources, including social media and digital platforms, often accelerated by AI-driven amplification, contributing to public panic, incite political violence, increase social tensions and hampering emergency response^[3].

This is not a security failure by governments; it is an inherent vulnerability of open digital societies in crisis. Civilians cannot be expected to know what information is operationally sensitive or not. The intention is very often to share what they are witnessing and experiencing.

1. Abedin et. al, 2025, "A Call to Arms: Automated Methods for Identifying Weapons in Social Media Analysis of Conflict Zones", Websci <25, web-link/DOI: <https://dl.acm.org/doi/10.1145/3717867.3717886>

2. Andrew N. Liaropoulos, 2023, "Victory and Virality: War in the Age of Social Media", Published by Johns Hopkins University Press, web-link/DOI: <https://doi.org/10.1353/gia.2023.a913646>

3. Kelly M Greenhill and Ben Oppenheim , 2017, "Rumor Has It: The Adoption of Unverified Information in Conflict Zones", Journal of International Studies Quarterly, web-link/DOI: <https://doi.org/10.1093/isq/sqx015>

III GPS Jamming and Navigation Disruption

In recent conflicts, widespread GPS interference has been confirmed in and around major maritime routes. In some regions, reports indicate that within a single 24-hour period, more than 1,100 vessels reported GPS signal disruption, causing navigational inaccuracy in some of the world's most critical and commercially significant shipping corridors ^[1].

+1,100

vessels reported GPS signal disruption



Civilian aviation in affected areas has also experienced significant navigational disruption, compounding the risks for commercial flight operations.

The risk of maritime accidents and aviation incidents as a direct result of this disruption is significant and ongoing.

Civilian populations dependent on goods transported through affected shipping routes, as well as the integrity of civilian digital ecosystems, are also exposed to secondary economic and supply-chain impacts.

IV Deliberate attacks on Civilian Digital Infrastructure

Incidents affecting critical civilian infrastructure and digital services such as government websites, airport information systems platforms, banking portals, and telecommunications providers.

The cumulative effect on public confidence and access to government digital services is significant, particularly at a moment when accurate, timely official communications are most needed.

In addition, large-scale destructive cyber incidents on civilian critical infrastructure, such as power grids, hospitals, food supply management or water systems, could directly disrupt civilian digital ecosystems. The threat level could elevate, and Governments should maintain heightened caution.

In response to these evolving digital threats, the report outlines a set of recommendations and calls to action across priority areas to enhance the protection, resilience, and continuity of civilian digital ecosystems during crises.



C. Recommendations and call for action

8 This section provides the details of the proposed actions, grouped into tracks, to be considered by stakeholders in their deliberations to address the affecting civilian digital ecosystems during crisis.

Considering the categories or threats as well as the emerging digital-related risks to be considered, the DCO Secretariat recommends facilitating further cooperative discussions focusing on 4 priority areas (Tracks) to safeguard the civilian digital ecosystem:

- 01 Ensure the Resilience of the Civilian Digital Infrastructure.
- 02 Protect and Build Public Trust.
- 03 Share Emergency Knowledge and Information.
- 04 Ensure Digital Services Continuity and Resilience.

For each priority area, this report lists a comprehensive list of actions to be taken by the relevant stakeholders.

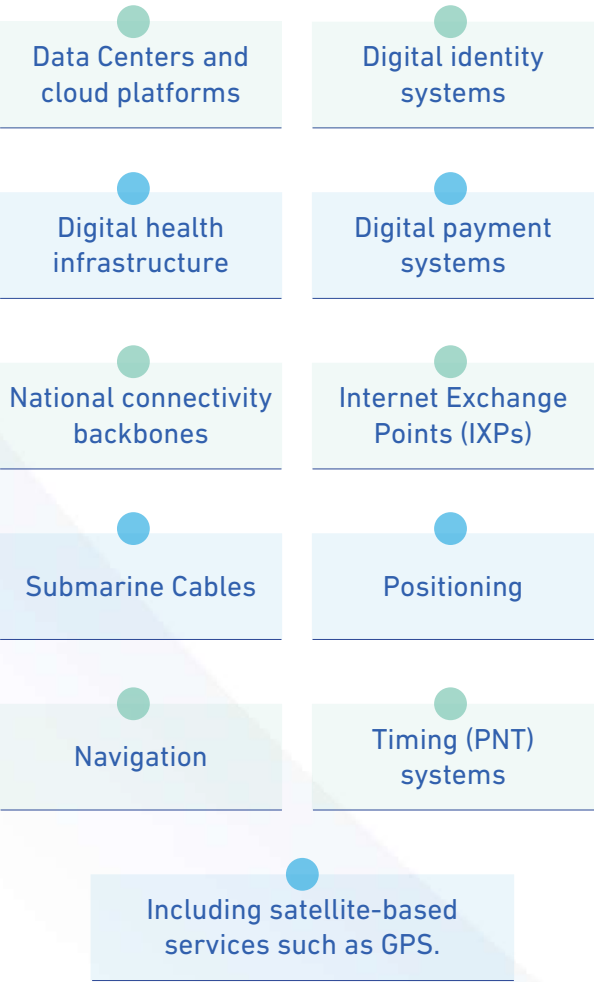
1. Organized Crime and Corruption Reporting Project (OCCRP) : <https://www.occrp.org/en/news/more-than-1100-ships-hit-by-widespread-gps-disruption-after-iran-strikes#:~:text=Reported%20by,overpower%20the%20legitimate%20GPS%20signals.>

Track 1: Ensure Resilience of Civilian Digital Infrastructure

Civilian digital infrastructure underpins essential public services and economic activity. During Crisis, disruptions to digital infrastructure can have significant and severe consequences for civilian welfare, public safety, and emergency response capabilities.

1.1 Physical and Shared Connectivity Infrastructure

Governments may wish to recognize that the resilience of civilian digital ecosystems, including digital access, relies on physical infrastructure that is often shared, cross-border, and largely invisible to policymakers until it fails. This infrastructure includes but is not limited to:



The following components warrant particular attention:

Submarine Cables:

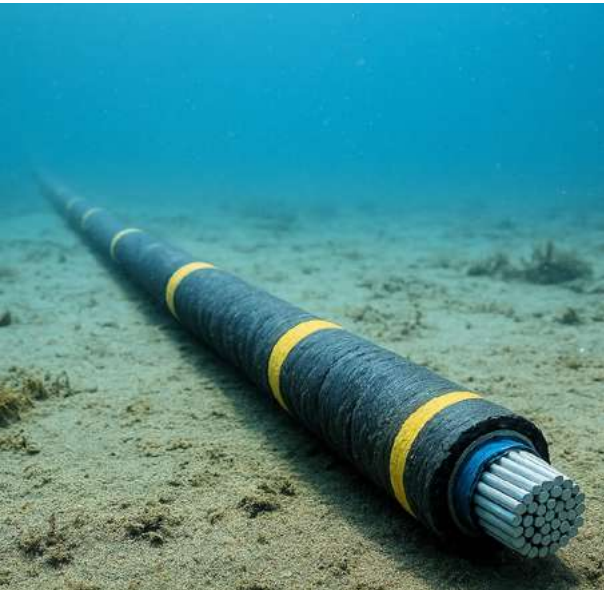
Submarine cables carry roughly 95% of global data traffic, including the communications and commercial transactions of every government, and are critical to the functioning of civilian digital ecosystems.

Submarine cables carry roughl

95%

global data traffic

These cables are concentrated at a limited number of coastal landing stations, creating areas of concentrated exposure.



Available reports and observed incidents in different regions indicate that submarine cable infrastructure may be exposed to physical interference or disruption, demonstrating that these assets are not safeguarded by their remoteness or apparent inaccessibility.

Stakeholders, particularly governments are encouraged to:

- 01 Assess national dependence on submarine cable routes and their coastal landing stations.
- 02 Engage in regional coordination to protect shared cable infrastructure and landing stations.
- 03 Establish contingency routing plans and maintain satellite backup capacity for critical government and emergency services; and
- 04 Ensure that cable landing stations are formally recognized as as part of critical national infrastructure frameworks and provided with appropriate physical and legal protection.

Positioning, navigation, and timing (PNT) systems,

Including satellite-based services such as GPS perspective, governments, in-consultation with stakeholders should:

- 01 Develop contingency measures for navigation and timing disruptions, including backup navigation protocols and access to alternative or complementary PNT systems.

Internet Exchange Points (IXPs):

Internet Exchange Points (IXPs) are facilities where different telecommunications networks interconnect to exchange traffic, often located in data centers, co-location facilities, or other secure network hubs.

They enable efficient and resilient interconnection of multiple internet service providers and play a key role in determining the efficiency and independence of national internet traffic flows.

In the absence of a functioning IXP, a country may become more dependent on routing domestic internet traffic through external networks, creating dependencies that are difficult to manage during a crisis. Despite their critical importance, IXPs ot always formally recognized within national critical infrastructure frameworks.

Governments and relevant stakeholders are encouraged to:

- 01 Consider the inclusion of IXPs within national critical infrastructure planning frameworks, supported by appropriate governance and protection measures
- 02 Ensure IXPs are equipped with redundant power systems, physical security, and network diversity; and
- 03 Develop regional IXP cooperation frameworks to maintain connectivity in the event that a national IXP is disrupted.



Energy Resilience for Digital Infrastructure:

Digital infrastructure, including data centers, IXPs, mobile towers, and exchange points, requires uninterrupted power to operate.

Power disruptions, whether caused by external shocks or broader infrastructure failures, cascade directly into communications blackouts and undermine the stability of civilian digital ecosystems.

Governments and relevant stakeholders are encouraged to:

- 01 Require operators of critical digital infrastructure to maintain backup power systems capable of sustaining operations through extended outages, and to test these systems on a regular basis.
- 02 Strengthen regional energy resilience by exploring cross-border electricity support mechanisms and coordination arrangements with neighboring countries and their local stakeholders, enabling emergency power supply or grid support during major disruptions.
- 03 Plan for diversified and decentralized power sources for critical digital infrastructure, including renewable energy with battery storage or microgrid solutions, to reduce reliance on single power supply pathways; and
- 04 Support the inclusion of the key digital infrastructure within national electricity restoration planning, ensuring that telecommunications networks, IXPs, and major data centers are restored rapidly following power disruptions.



1.2 Alignment with International Humanitarian Principles

Governments and relevant stakeholders are encouraged to:

- 01 Advocate for the protection of civilian digital infrastructure in line with internationally recognized humanitarian principles.
- 02 Support multilateral discussions within relevant United Nations bodies and other international forums addressing responsible government behavior in cyberspace; and
- 03 Promote broader international recognition of the importance of digital infrastructure for civilian protection and continuity of essential services during crisis.

1.3 National Policy and Legal Measures

Governments and other stakeholders may consider:

- 01 Considering the inclusion of digital infrastructure within national critical infrastructure frameworks.
- 02 Establishing legal safeguards against targeting, misuse, or disruption of civilian digital ecosystems; and
- 03 Integrating digital resilience into national civil defense and emergency preparedness strategies.

Track 2: Protect and Build Public Trust

During crisis, access to accurate and trusted information is essential for civilian safety, maintaining confidence in information sources, and enabling effective emergency response. Disruptions to official communication channels, manipulation of emergency information, or the spread of unverified content can create confusion and undermine crisis management efforts.

Strengthening the protection of official crisis communication channels and promoting responsible digital behavior among the public are key measures for maintaining trusted information environments and reducing risks to both civilians and emergency responders.



2.1 Protection of Official Communication Channels

Official communication channels used during emergencies serve as primary sources of verified information for civilians and institutions. Safeguarding their integrity, authenticity, and availability of these channels is essential to ensure that accurate and timely information reaches the public.

Governments and relevant stakeholders are encouraged to:

- 01 Safeguard official communication channels used during crises, including official portals, emergency alert systems, and verified social media accounts.
- 02 Apply authentication and verification measures, including digital signatures and content integrity standards to official communications, so that their origin can be independently verified.
- 03 Strengthen cybersecurity protections for crisis communication platforms to prevent hacking, impersonation, or manipulation of official information.
- 04 Coordinate with digital platforms and online service providers where appropriate, during crises to help address misleading content that impersonates official authorities or manipulated emergency communications.
- 05 Implement mechanisms enabling stakeholders, including civilians to verify the authenticity of critical public service announcements, including verified accounts and centralized government information portals; and
- 06 Promote coordinated communication across agencies to ensure consistent and trusted messaging during emergencies.

2.2 Public Awareness and Responsible Digital Behavior

During crisis individuals may unintentionally contribute to the spread of sensitive or misleading information via digital platforms. Real-time sharing of images, videos, or locations data on social media may inadvertently reveal information related to emergency situations, civilian presence, or essential public infrastructure.

Governments and relevant stakeholders are encouraged to promote public awareness initiatives that emphasize:

- 01 Responsible information-sharing during crises, including verifying information before sharing digital content.
- 02 Avoiding real-time posting of sensitive locations, situations, or movements that may unintentionally expose civilians or responders to risk.
- 03 Supporting digital literacy initiatives that help individuals identify manipulated or misleading digital content.
- 04 Engaging civil society, media organizations, and digital platforms in promoting responsible information-sharing practices; and
- 05 Promoting responsible digital behavior as a key element of societal resilience and civilian protection during periods of crisis.

2.3 Responding to AI-Enabled Online Misinformation and Disinformation

The current crisis environment demonstrates that, beyond conventional online misinformation and disinformation, AI-generated content introduces a new level of digital risks that is increasingly present in real-world contexts, shaping public perception of events in ways that can directly affect civilian safety and destabilize civilian digital ecosystems. Policy responses must therefore match the speed, scale, and technological sophistication of this evolving risks.

Governments and relevant stakeholders are encouraged to:

- 01 Establish rapid-response misinformation and disinformation capabilities: Designate, within an existing multi-stakeholder body or as a dedicated unit, a rapid-response capacity for detecting and countering AI-generated misinformation and disinformation affecting the national information environment. This function should be operationally ready prior to crises, enabling timely response during emergencies.
- 02 Pre-negotiate crisis protocols with digital platforms: Develop advance coordination mechanisms with major social media and digital platforms in advance of crises, including agreed procedures for rapid escalation of harmful online content, mitigation of amplification risks, and coordinated counter-messaging. These mechanisms must be in place before they are needed; and
- 03 Require digital platform transparency: Encourage digital platforms operating under relevant national jurisdictions to support transparency measures related to AI-generated content in conflict contexts and to provide national authorities with regular transparency reporting on the scale and nature of crisis-related content manipulation.

Track 3: Share Emergency Knowledge and Information

Governments and relevant stakeholders individually and collectively face significant challenges in addressing the digital risks posed by crisis. The current crisis landscape impacts multiple Governments simultaneously, placing increasing pressure on civilian digital ecosystems.

The knowledge, tools, and experience needed for an effective response are distributed across the Governments, making coordinated action the most effective approach. Facilitating rapid, trusted, and structured information exchange among Governments can therefore strengthen response efforts and help mitigate disruptions to civilian digital ecosystems.



3.1 Establish Rapid Coordination Channels

Governments and relevant stakeholders are encouraged to:

- 01 Designate focal points for digital resilience coordination.
- 02 Participate in emergency coordination calls or trusted information exchange mechanisms facilitated through multilateral platforms.
- 03 Share situational assessments regarding digital infrastructure disruptions affecting essential public services; and
- 04 Develop and implement with relevant stakeholders early awareness and alert mechanisms leveraging digital platforms and real-time monitoring systems to enable rapid communication of emerging digital risks or disruptions before they propagate across Governments.

3.2 Exchange of Best Practices in Critical Areas

Governments and relevant stakeholders are encouraged to exchange best practices in areas including:

- Data Backup and Redundancy:**
 - Off-site and geographically distributed backups;
 - Offline backup protocols;
 - Immutable backup systems; and
 - Regular testing of recovery mechanisms.
- Cross-Border Hosting Arrangements:**
 - Pre-agreed emergency hosting arrangements with trusted legal entity, policy and legal arrangements to enable continuity of critical data services during emergencies; and
 - Digital Sovereignty safeguards for externally hosted public data.



Cloud Failover Strategies:

- Multi-region and multi-cloud deployment architectures;
- Automated failover configurations; and
- Service continuity protocols for essential digital systems.

Satellite and Alternative Connectivity:

- Satellite backup connectivity for essential public services;
- Mobile emergency communication units; and
- Diversified network pathways for resilient connectivity.

Cybersecurity Threat Intelligence Sharing:

- Technical indicators of cyber incidents (e.g., early signs of system compromise).
- Incident response strategies;
- Coordinated technical guidance during cybersecurity incidents; and
- Lessons learned from infrastructure recovery efforts.

Track 4: Ensure Digital Services Continuity and Resilience

Ensuring the continuity of essential digital services during crisis is critical to protecting civilian welfare and maintaining the functioning of core public institutions. Preparedness planning, redundancy mechanisms, and effective governance frameworks help ensure that civilian digital ecosystems supporting essential and critical public services and crisis communication remain operational.

4.1 Minimum Digital Service Continuity Framework

Essential digital services, including emergency communications, health information systems, civil registry, financial transaction systems, and humanitarian aid coordination, and services dependent on positioning, navigation, and timing (PNT) systems shall be maintained or restored during crisis to safeguard civilian digital ecosystems.

Disruptions to these services are far more than an inconvenience, as they can directly affect people's ability to access medical care, receive emergency assistance, or communicate with their family.

Governments and relevant stakeholders are encouraged to:

- 01 Define a minimum Digital Service Continuity Framework prioritizing digital services essential to civilian welfare and emergency coordination that must remain operational during crisis and prioritize their protection accordingly. Priority services may include:
 - Healthcare information systems.
 - Civil registration and digital identity services.
 - Payment systems and social protection platforms.
 - Emergency communication and public information systems; and
 - Utility management systems.

- 02 Pre-position backup systems, including geographically distributed and securely hosted copies of critical data and services to allow rapid restoration if primary systems are disrupted.
- 03 Ensure continuity of services dependent on positioning, navigation, and timing (PNT), including through backup navigation protocols and alternative or complementary PNT systems; and
- 04 Establish tested continuity-of-operations plans for digital services that can be activated within a timely manner following a major disruption.



4.2 Business Continuity and Disaster Recovery Planning

Governments and relevant stakeholders may strengthen:

- 01 Digital business continuity plans for essential services.
- 02 Integrated disaster recovery and resilience strategies for essential digital infrastructure and public communication systems, where appropriate.
- 03 Regular simulation exercises to test system resilience and preparedness and response readiness of essential digital services;
- 04 Affecting digital infrastructure and essential services;
- 05 Inter-agency and multi-stakeholder coordination mechanisms for responding to significant disruptions affecting essential digital services;
- 06 Incorporate contingency measures for GPS and other PNT disruptions, including fallback navigation protocols and complementary and resilient timing and positioning solutions where applicable, into continuity and disaster recovery plans; and
- 07 Crisis governance structures responsible for maintaining continuity of essential services and trusted public communication channels, during major disruption events, ensuring coordination, clarity of roles, and continuity of public information flows.

4.3 Data Governance During Conflict

Crisis introduces heightened risks to personal and sensitive data. Governments and relevant stakeholders are encouraged to:

- 01 Maintain data protection safeguards for personal and sensitive information, including civil registry and digital identity data even during emergency situations.
- 02 Establish emergency data-sharing protocols that respect privacy, security, and responsible data governance.
- 03 Protect sensitive registries, particularly civil registration and digital identity systems, from risks affecting integrity, availability, or secure operation.
- 04 Maintain audit trails during system migration, backup restoration, or infrastructure recovery; including for civil registry and identity data systems; to support accountability and system integrity during recovery processes; and
- 05 Protecting civilian data is essential to maintaining public trust and confidence in digital public services.

D. DCO Initiatives and program support safeguarding efforts during crisis

9 This advisory supports governments and relevant stakeholders in safeguarding civilian digital ecosystems during crisis by enabling evidence-based decision-making, coordinated action, and access to practical tools and partnerships that strengthen resilience and continuity of essential services.

10 At the center of this support is the Digital Economy Navigator (DEN), which provides a baseline to identify critical vulnerabilities, and prioritize response measures. Through its analytical capabilities and simulation features, DEN enables stakeholders, including governments to anticipate disruptions, allocate resources effectively, and accelerate implementation of the Advisory's recommended actions.



11 The DCO complements this diagnostic foundation with impact-oriented initiatives that support governments and relevant stakeholders across key priority areas. DCO initiatives are cross-border by design and can help fostering cooperation.

To reinforce the continuity of essential services, DCO facilitates access to tested digital solutions and peer support through the IMPACT Platform, while the Cross-Border Data Flow Initiative and DCO Privacy Principles provide operational mechanisms and legal tools to enable trusted data exchange arrangements, supporting cross-border service continuity in crisis context.

12 To strengthen trust and risk management, the DCO can provide governments and relevant stakeholders with practical governance tools such as the AI-REAL Toolkit and AI Ethics Evaluator, while advancing coordinated approaches through the Online Content Integrity initiative to counter with AI-enabled Online Misinformation and Disinformation, ensuring more reliable public communication during crises.



13 In parallel, the DCO supports economic continuity through initiatives such as the Digital Foreign Direct Investment (DFDI) Initiative, alongside the Model Digital Economy Agreement (MDEA) to sustain cross-border digital trade, and the Model Startup Act (MSA) and Scale-up Trusted Resources for Innovation Driven Enterprises (STRIDE) to strengthen startup ecosystems and entrepreneurship resilience. Additional DCO initiatives are designed to further reinforce governments eco-system at human level, including the Skills Universe, which expands access to critical digital skills; and WE-Elevate, which supports women-led Micro, Small, and Medium Enterprises (MSMEs) and inclusive economic participation.

14 A key strength of the DCO lies in its multi-stakeholder ecosystem. DCO Observers and partners can support the provision of localized and decentralized digital capabilities, helping ensure service continuity while reducing reliance on external or centralized digital systems that may present single points of failure in times of crisis.

E. Call for action and timeline

15 Strengthened cooperation among stakeholders remains essential to collective resilience. In this regard, governments and relevant stakeholders are encouraged with the support of the international organizations, to review the proposed action, prioritize tracks and activities, and coordinate next steps. In addition, impacted governments and other relevant stakeholders can strengthen mechanisms to share technical assistance, operational expertise in infrastructure protection and crisis communication, and to exchange information and knowledge.

16 The following recommended next steps will provide a structured framework for government relevant stakeholders to safeguard civilian digital ecosystems durin crisis and ensure higher resilience in case of future hostile events:

Short-Term Action (1-3 months)

- 01** Establish AI-enabled monitoring mechanisms to detect and counter online misinformation and impersonation of official multilateral channels.
- 02** Establish rapid-response capabilities to help identify, assess, and address AI-driven misinformation and disinformation in a timely and coordinated manner.
- 03** Identify and prioritize essential digital services for continuity, including healthcare, payments, and emergency alerts.

- 04** Develop crisis communication and escalation protocols with major social media and digital platforms to address harmful or manipulated online content during emergencies.
- 05** Create a shared depository of critical digital infrastructure for governments at global, regional, and national levels.
- 06** Identify solutions for cross-border infrastructure redundancy, backup power, and alternative digital connectivity.
- 07** Strengthen collaboration among stakeholders, including governments to facilitate the exchange of good practices and lessons learned on digital infrastructure resilience and the continuity of essential services.



Medium-Term Actions (3–12 months)

- 01 Develop national digital continuity and resilience frameworks for essential digital services, in collaboration with relevant stakeholders across the public and private sectors.
- 02 Strengthen protection and resilience measures for critical digital infrastructure (such as Internet Exchange Points, data centers, and submarine cables), in accordance with national frameworks and applicable laws.
- 03 Implement distributed backups, resilient cloud recovery and failover capabilities, and geographically distributed hosting and secure redundancy solutions, where appropriate.
- 04 Conduct simulations and regional exercises to test cyber-incidents, digital infrastructure, data governance, positioning and timing disruptions, digital connectivity, and information resilience.
- 05 Develop contingency measures for GPS disruption, including backup navigation protocols and diversified and resilient positioning, navigation, and timing (PNT) solutions.

Long-Term Actions (>12 months)

- 01 Encourage multi-stakeholder investment approaches to develop diversified connectivity, resilient power, and redundant infrastructure.
- 02 Promote international norms recognizing the importance of safeguarding civilian digital ecosystems and ensuring their resilience.
- 03 Strengthen multilateral cooperation to address risks related to content integrity in digital and AI-enabled environments.
- 04 Institutionalize multilateral support mechanisms and conduct regular resilience and preparedness assessments.
- 05 Promote the institutionalization of multilateral digital solidarity mechanisms that facilitate technical assistance and temporary digital infrastructure support among governments and stakeholders during crises.

F. Conclusion

17 The protection of civilians has long been a foundational obligation of international law. In an age where critical services — from healthcare and finance to emergency response and civil administration — operate through digital systems, that obligation must be applied with equal force to the digital realm. Major disruptions can affect not only physical infrastructure but the entire digital fabric of daily governance and civilian life.

18 The four strategic tracks set out in this report — resilience, trust, knowledge sharing, and service continuity — provide governments with a clear, actionable framework to fulfil that obligation. These tracks are not aspirational principles; they are practical, implementable commitments, many of which can be initiated promptly.

19 The timeliness of this report reflects the urgency of the moment. Disruptions can be sudden and complex and preparedness cannot wait for a crisis to materialize. Governments and other relevant stakeholders that act now—by securing communications, classifying digital infrastructure as protected assets, and building cross-border redundancy—will be more resilient in their ability to protect their populations and maintain essential services when it matters most.

20 The DCO calls on all relevant stakeholders, including governments, to act on the findings of this report as a basis for immediate collective action. The DCO stands ready to support stakeholders through data-driven insights, practical policy guidance, and digital tools, such as the Digital Economy Navigator (DEN), Digital Foreign Direct Investment (DFDI), WE-Elevate Initiative, and AI-REAL Toolkit, and its multi-stakeholder ecosystem, including Observers and Partners who can contribute decentralized and diversified digital capabilities and operational support. Safeguarding civilian digital ecosystems is a shared responsibility. Meeting it requires shared resolve.

Disclaimer

This report is issued by the DCO General Secretariat as guidance to support the stakeholders in safeguarding civilian digital ecosystems, and it does not create legal obligations for DCO and its Member States. References to digital risks are illustrative only and not intended to attribute responsibility to any specific actor, while stakeholders, including governments retain full sovereignty in determining implementation of recommendations. The DCO remains neutral in all contexts and disclaims liability for reliance on this advisory, emphasizing that all cooperative measures are voluntary and subject to national discretion. This report may contain findings, interpretations, or recommendations that do not necessarily reflect the views of the DCO. Its contents may be updated, amended, or withdrawn at any time without prior notice.



Follow us on

   @dcorg |  www.dco.org

© 2026 The Digital Cooperation Organization