CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

NOVEMBER 2023

Emergency Management and Information Integrity: A Framework for Crisis Response

Iryna Adam, Samantha Lai, Arthur Nelson,
Alicia Wanless, and Kamya Yadav

Emergency Management and Information Integrity: A Framework for Crisis Response

Iryna Adam, Samantha Lai, Arthur Nelson,
Alicia Wanless, and Kamya Yadav

Carnegie's Partnership for Countering Influence Operations is grateful for funding provided by the Government of Canada, the William and Flora Hewlett Foundation, Craig Newmark Philanthropies, the John S. and James L. Knight Foundation, Microsoft, Meta, Google, Twitter, and WhatsApp. The PCIO is wholly and solely responsible for the contents of its products, written or otherwise. We welcome conversations with new donors. All donations are subject to Carnegie's donor policy review. We do not allow donors prior approval of drafts, influence on selection of project participants, or any influence over the findings and recommendations of work they may support.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Summary

Mitigating the negative impacts of crises on the information environment is a significant challenge for democracies, especially as the frequency and severity of violent conflicts and natural disasters rise worldwide. Drawing on lessons from Russia's invasion of Ukraine, **this paper explores how well-established emergency management concepts can help government policymakers effectively combat efforts to undermine information integrity in the next crisis.**

The Partnership for Countering Influence Operations at the Carnegie Endowment for International Peace operated a crisis response network of fifty-four government agencies, tech companies, and civil society organizations (CSOs) working to protect the Ukrainian information environment over the last year.[1] Drawing on eleven months of documented operations, including fifty-seven needs assessments and original datasets of publicly disclosed interventions by G7 Rapid Response Mechanism (RRM) members and observers and major tech companies, we observed several consistent **challenges with coordination, defining success, inflexible funding models, and siloed operations across stakeholders, including government, industry, civil society, and media**. A formalized emergency management plan would have enabled better coordination across stakeholders to address those issues.

The aim of emergency management for the information environment should be the protection of society by preserving information integrity—a measure of the consistency, reliability, accuracy, fidelity, safety, and transparency of an information ecosystem—to provide a roadmap for actions democracies can take to protect the information environment. Interventions should be planned before, during, and after a crisis, across four phases:

prevention & mitigation, preparedness, response, and recovery. This framework can improve democracies' ability to intervene during a crisis by:

- Instilling a shared aim among stakeholders, specifically to preserve information integrity
- Providing a means of constructive coordination between stakeholders
- Helping decisionmakers identify and prioritize capacity-building needs in democracies, including the unexpected like natural disasters
- Ensuring funding models sustain essential nonprofit organizations in a crisis
- Enabling systemic thinking to bridge siloes and divides that inhibit coordination

What should governments do? Develop an information integrity-based emergency management framework. Democracies should identify and map the range of options for intervention in the information environment across departments and agencies of member and observer countries to better understand what is collectively possible. This enables governments to improve democracies' ability to reduce the loss of and restore information integrity during a crisis.

Introduction

Democracies worldwide are struggling to respond to crises in large part due to a complex and polluted information environment.[2] Mitigating the negative effects of foreign information manipulation and interference on the information environment in democracies is a particular challenge for policymakers. Such crises tend to generate a spike in information pollution and a loss of information integrity as people try to make sense of the situation, while rumors, disinformation, and outright scams abound.[3] From COVID-19 misinformation to authoritarian crackdowns on democratic protests or hybrid warfare involving information manipulation, the negative impacts that crises have on the information environment can be challenging to reverse, threatening the physical safety of civilians and the democratic stability of societies.

The stakes will continue to grow in the face of more frequent and severe crises—the world is experiencing a surge in global protests and internet shutdowns, a spate of natural disasters and climate shocks, and the highest rate of violent conflicts since World War II.[4] Now more than ever, democracies must find a structured approach to guide interventions within the information environment, based on a clear and familiar framework outlining activities that

must be developed, exercised and resourced in advance. This paper, based on lessons accumulated during a multistakeholder pilot project aiming to assist Ukraine during the continuing Russian war of aggression, offers a starting point to frame multistakeholder dialogue for coordinating responses in the information environment in the context of democracies. In so doing, it provides a shared vision for action around a concept of information integrity, and a framework for planning interventions based on emergency management.

Experiences in Ukraine

Russia's further invasion of Ukraine was an unprecedented test of how a multistakeholder coalition can work to collectively ensure the information integrity of a country in crisis. Governments, tech companies, civil society organizations, and other actors surged to protect the Ukrainian information ecosystem. These fast yet often disparate responses helped Ukrainians maintain access to essential information at the outset of the invasion and kept people outside of Ukraine informed and capable of modulating their responses accordingly. To support these efforts, the Carnegie Endowment for International Peace's Partnership for Countering Influence Operations (PCIO) established a multistakeholder crisis response network called Info Integrity Ukraine (IIUA). The aims of the project, supported by Global Affairs Canada and in partnership with the NATO Strategic Communications Centre of Excellence, were to facilitate multistakeholder coordination to address immediate conflict needs and identify lessons learned to improve multistakeholder responses to future crises.

This paper explores how an emergency management approach to a crisis unfolding partly in the information environment can help policymakers plan and structure interventions and responses. This framework provides a path for planning interventions and responses before, during, and after a crisis hits. It focuses primarily on what democratic governments can do on both domestic and international levels to develop a multistakeholder crisis response guided by principles of information integrity. The same framework can be applied by social media companies and civil society organizations.[5]

Emergency management is only one of many approaches to develop capacity related to information integrity, and shares connections to other fields like critical infrastructure protection and community capacity building. The approaches detailed in this paper should be part of a larger picture and complement other initiatives working toward breaking down siloes and enhancing cooperation.

Ukraine poses its own limitations as a case study. Following the 2014 invasion of Crimea, Ukraine's government stepped up their involvement in protecting the information environment. Prior to Russia's invasion in 2022, the country already had programming in place and

a well-trained and reasonably organized civil society. This will not be the case for all other countries. However, Ukraine's preexisting capacity is also a lesson for how other countries can build capacity to address future crises.

Case Study: Building a Case Against Russian War Propaganda

As part of IIUA efforts, PCIO supported an initiative aimed at building a case to prosecute Russia on the use of war propaganda to incite aggression against Ukrainians. Russia's actions are in violation of Article 20 of the International Covenant on Civil and Political Rights, which mandates that any "advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence shall be prohibited by law."[6] This single example demonstrates how issues within the information environment span silos and mandates, and require a systematized approach to planning for, prioritizing, and executing various activities, highlighting the need for taking a multistakeholder response when intervening within it.

Sadly, the need for building such a case begins in the physical world with systematic violence against a population. There will be civilian victims and witnesses that lead to documentation. Sometimes this means the involvement of mainstream media coverage—and there are all stripes of media stakeholders from independent media who, in a country like Ukraine, are often supported by media development agencies in democracies, but there are also for-profit outlets and state-run media. Increasingly, civilians are directly documenting war crimes using their cell phones made by private companies, and using applications that are offered through app stores. Some will post to social media, again controlled mainly by the private sector. Others might use apps built by nonprofits like eyeWitness, which are usually supported by democratic government granting programs.

In the documentation of war crimes, infrastructure issues emerge—can these witnesses access the services necessary to collect evidence? Is there electricity, is there internet access? The very act of documenting war crimes can put civilians at risk, which brings in issues of digital safety.

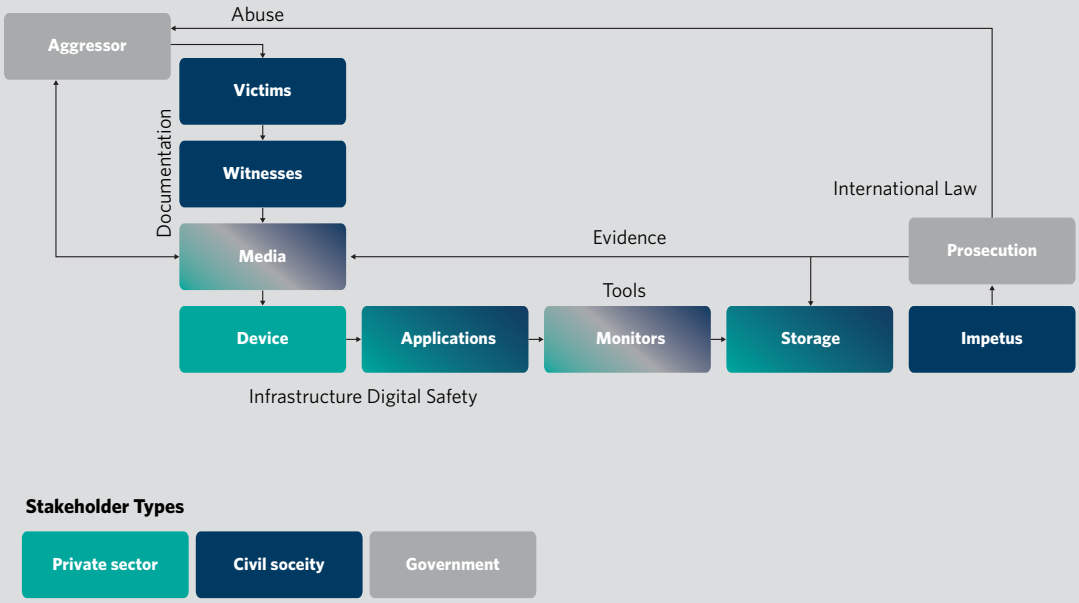
In addition to those documenting war crimes, there are many other stakeholders monitoring and investigating what evidence is shared of those crimes and what propaganda messaging might have incited them. These stakeholders run the gamut from civil society organizations to teams inside government agencies and private sector companies.

All this evidence gets stored not just on devices, social media platforms, and cloud services, but also in storage lockers built to help document evidence. While major online services tend to be run by private companies, evidence lockers are built and managed by nonprofits, such as Mnemonic, who again are supported by a host of different granting programs including democracies and philanthropies.

Typically, for a case to be brought forward, there needs to be impetus. Depending on who the aggressor is, that might be the local government, but is almost always civil society, and both stakeholder types need the interest of the International Criminal Court. However, cooperation of tech companies is often required to get evidence, although they might have deleted content that could have been brought forward as evidence. Evidence can also be found in media coverage and public statements. The ultimate aim in all of this effort is to prove that the aggressor was involved in provoking people to commit war crimes.

If we evaluate this from a whole-of-society perspective, prosecuting war crimes involves civil society, government, and the private sector. It also cuts across numerous mandates, including issues related to infrastructure, security, disinformation, and international law.

Figure 1. Why Systemic and Multistakeholder: Building a Case Against Russian War Propaganda



Source: Authors' research.

Given PCIO's role in connecting many of these stakeholder types in the pursuit of building a case to demonstrate that Russia engaged in war propaganda to incite violent aggression against Ukrainians, we can say conclusively that had there been an emergency management framework in place, these efforts could have been significantly expedited and more efficient. Instead, it required the identification of a gap via the needs assessments and prior experience with a variety of stakeholders in another conflict (Syria) to connect these dots.

A Framework for Crisis Response

Information Integrity as a Guiding Principle

A key lesson emerging from the IIUA was that many stakeholders wanted a clearer definition of success to guide efforts to protect the information environment. Information integrity as a framework can provide a shared idea of success, outline objectives, and articulate operating principles in line with democratic values. That said, the concept needs further development to offer stakeholders a guide.

Information integrity is a concept from the field of information security that is increasingly being applied to the information environment by policymakers.[7] In the information security field, information integrity relates to activities aimed at enhancing and securing the accuracy, consistency, and reliability of information in a closed information system, although others working more on disinformation have begun to adopt the term. This concept works in the context of an organization's computer network, for example. The information environment, of course, is far more complex, comprising multiple technologies, different types of information, and billions of people. Moreover, the information environment in democracies is supposed to be inherently open and free. In the context of democracies, information integrity can be conceptualized through six criteria:

- **Consistency:** The regularity or steady continuity of access to information including the ability to stay online and the maintenance and functioning of infrastructure. In Ukraine, efforts in this category included enhancing connectivity, such as tech companies and governments donating hardware (for example, Starlink).

- **Reliability:** The suitability of results regarding information including enabling quality sources of information and media sources that are sustainable, independent, and transparent. Examples of efforts supporting reliability in Ukraine included additional financial, intellectual, and material support for media development organizations.

- **Accuracy:** The quality or state of information being correct or precise, including efforts in fact-checking and disinformation monitoring. Efforts in this category were among the most prevalent in Ukraine, including numerous well-coordinated fact-checking initiatives both in Ukraine and across Europe; efforts that amplified credible and useful information, such as tech companies promoting content from trusted local media outlets to reach local target groups; and the enforcement of policies by tech companies to remove coordinated inauthentic activity and manipulative behavior from platforms.

- **Fidelity:** The degree of exactness with which information is copied or reproduced, or in the context of the information environment the degree to which audiences understand information as originally intended by the producer/sender. This category includes media literacy efforts and pre-bunking. While this category is the most challenging to measure for impact, as it requires understanding how audiences receive and process information, it was a well-covered area in Ukraine, specifically given long-standing issues with Russian disinformation and propaganda.

- **Safety**: The condition of being protected from or unlikely to be at risk of danger or injury. This could include digital safety and cybersecurity, which in the context of Ukraine, meant tech companies and governments providing key Ukrainian government actors with off-the-shelf cybersecurity capabilities (for example, software licenses, DDoS protections).

- **Transparency:** The quality of work being done in an open way without secrets. This relates to stakeholders being accountable and transparent about how they engage with each other in crisis response. In the context of Ukraine, this includes government agencies communicating with industry and civil society on what they have been doing and how decisions are being made.

This paper builds on accepted definitions of information integrity borrowing from the field of information/cyber security, to provide a roadmap for actions democracies can take to safeguard the integrity of the information environment. Stakeholders can work together to foster these core conditions and cultivate integrity in the information environment. Information integrity is easily undercut by chaos and confusion. In those times, people often look to public officials for reliable information and clarification. To undercut efforts to sow division in society, national governments need to develop a homogenous, coordinated response across departments and stakeholders to enable clarity. Similarly, the outlined criteria for information integrity should be the foundation for early warning monitoring and initial risk assessments. The ability to assess and classify the severity of any crisis is central to successful emergency management because it determines which resources and authorities will be allocated. The six criteria of information integrity should serve as the basis for developing such a severity classification scheme, including relevant qualitative and quantitative indicators and thresholds.

The information environment is complex and dynamic, and the effectiveness and the unintended impacts of interventions remain poorly understood. It will take collaborative effort and replicable measurements to understand what interventions are effective in combating efforts to undermine information integrity, without quashing a society's freedoms and plurality of voice. The goals set out could be achieved in a variety of ways, and the work needed will vary depending on the resources available, the levels of literacy among citizens and civil society, the accountability of the government, and the degree of trust citizens have in them.

The proposed framework specifically examines information integrity in the context of coordinating across multiple stakeholders during crisis response. The process of upholding information integrity might differ in how governments set conditions for information integrity outside of conflicts.[8]

Emergency Management is the Guide

While information integrity can provide principles, objectives, and measurements for interventions in the information environment in the context of democracy, a framework for organizing, prioritizing, and guiding those responses is still required. PCIO proposes to base these activities on a known framework already used in the physical environment.

Emergency or disaster management is a well-established framework that helps communities reduce vulnerability to hazards and cope with crises in the physical environment. Such crises consist of major disasters that a single community is not likely to handle on its own and to which the response requires broad-based engagement from individuals, households, organizations, and various levels of government.[9] The aim of emergency management is to avert a disaster and, where that is not an option, ensure a response that reduces damage as much as possible, as well as guiding recovery efforts to achieve *status ante*.

Public Safety Canada frames emergency management in four interdependent components or phases, namely: Prevention and Mitigation; Preparedness; Response; and Recovery.[10] The World Health Organization has also been exploring emergency management frameworks for combating what it calls infodemics in the wake of health crises.[11] Several countries also draw from the all-hazards approach, which lays out actions that stakeholders can take to prepare for a range of disasters.[12]

A similar approach can be applied to guiding responses to a crisis within the information environment, and provide a menu of options to guide interventions before, during and after a crisis:

- **Prevention and Mitigation**: Measures reducing risks in the information environment before a conflict erupts, such as having funding models in place that enable unexpected and rapid responses, short-term campaigns for general awareness-raising, or long-standing media literacy programs, as part of raising societal resilience to help reduce the public's susceptibility to disinformation. A federal government can consider additional activities under this rubric that focus on raising costs to adversaries, whereas public broadcasters and electoral commissions may develop programming that strengthens trust in democratic institutions and processes.

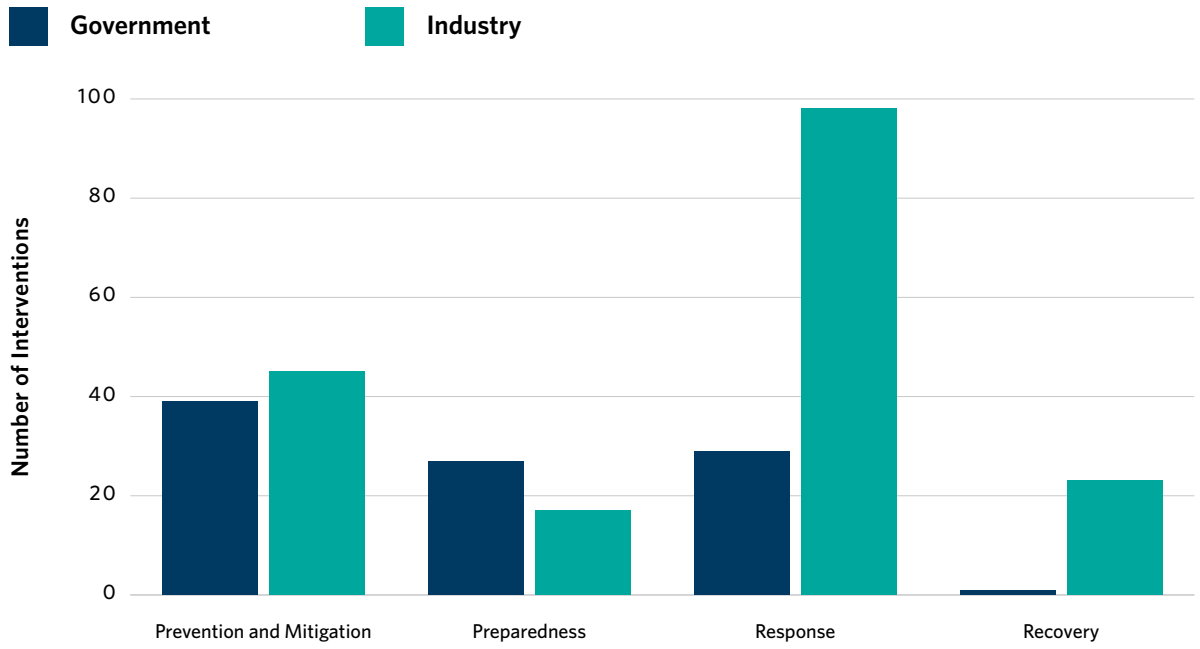
- **Preparedness**: Activities that ensure a response is possible such as training, procuring equipment, information sharing agreements across departments and other stakeholders, rules for making interventions that match the values of democracy, and fostering the capacity for intervention when the time comes. This includes coordinating donor and international organizations, governments, CSOs, media, and tech platforms to establish regular communication channels between stakeholders, as well as exercises and tabletops. Building these relationships and protocols creates capabilities for adaptive responses during times of crises.

- **Response**: The ability to act during or immediately before or after a conflict, or the interventions themselves, which currently dominate crisis response. In the context of Ukraine, this includes policy enforcements by tech companies, sanctions by governments, as well as the mapping and monitoring of Russian influence operations and targeted communities by all stakeholder types, to address the lack of structured exchange of different stakeholders' views of the current threat landscape.

- **Recovery**: Actions for addressing the aftermath of conflict. In the example of Ukraine, this includes shoring up independent media to rebound from revenue losses due to an affected economy in respect of competition and state aid rules, but also in pursuing justice on issues such as the use of war propaganda by Russia. Actions in the recovery stage should be planned prior to or from the outset of a crisis to ensure a response is possible. A successful recovery necessitates understanding and implementing activities that support Prevention and Mitigation efforts discussed above as well.

When PCIO mapped publicly disclosed interventions in support of Ukraine by four tech companies (Google, Meta, Microsoft, and X, formerly known as Twitter) and G7 RRM members and observers along an emergency management framework, it became apparent that more effort is needed in the pre-Response stages, especially in the Preparedness phase.

Figure 2. Types of Interventions During Russia's War on Ukraine



Source: Authors' calculations.

As mentioned, the data in the chart above is based on known activities during Russia's war on Ukraine. The uneven distribution of interventions across the stages demonstrates that stakeholders often lack a holistic approach to crisis management, which can dampen the effectiveness of the countermeasures deployed at the height of the crisis.

Collected data shows that both government and industry responses were heavily concentrated on the stage of Response, some in Prevention and Preparedness, with few initiatives focused on the Recovery period. Due to project closure ahead of the Recovery stage in Ukraine, PCIO was only able to collect limited data for this phase, but considerable anecdotal evidence demonstrates the need to start thinking about postcrisis interventions in earlier stages, and for there to be some degree of preparation for countries at heightened risk of imminent conflict. Few industry interventions fell into the Preparedness stage, an issue that could be mitigated in future crises, especially if industry partners are integrated into the framework. Industry might have had Preparedness initiatives, but little information was available publicly beyond existing policies, and other stakeholders seemed unaware. Addressing some of the problems that emerged at the Response stage at the start of and during the war would have allowed industry and actors on the ground to more smoothly cooperate, negating many of the misunderstandings and concerns about moderation policies that key stakeholders expressed during interviews.

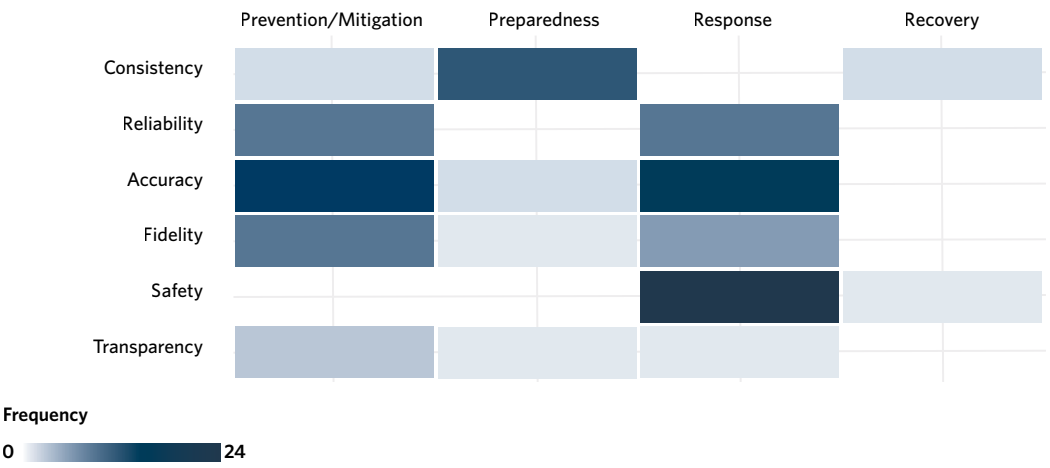
During the data collection process, stakeholders noted the lack of capacity building for media and CSOs on the ground. The lack of institutional investments in local organizations was a problem long before the war started. Independent media was less well-resourced, while oligarch-controlled media dominated most of the space. While there has always been an understanding of a need to build up strong and sustainable organizations with clear-cut policies and well-trained teams, this need has frequently taken a backseat to urgent issues, new short-term projects that gained the attention of donors and the international community, and high personnel turnover often caused by the previously mentioned nature of operating through short-term projects.

The consistent lack of investment in local civil society organizations is indicative of the piecemeal approach to crisis management. Capacity building is an important step in the Prevention stage, without which there are negative repercussions in further stages. It is, however, rarely prioritized as it does not show the immediate results that many organizations need to secure funding. Capacity-building activities are also defined differently across stakeholders, who then struggle to coordinate across priorities such as developing employees' skills, improving management, or increasing staff retention. Advancing a better understanding of what kinds of capacity are needed can guide stakeholders when setting priorities and donors and investors when selecting projects to support with less duplication and lower costs.

While hindsight is always 20/20, much of the inefficiency in Response could have been reduced with emergency management planning across stakeholder types in advance of and during the conflict. Indeed, such a coordinated response would be a massive step toward the often-touted concept of a whole-of-society approach.[13]

Areas in need of further development become clearer after plotting those publicly disclosed interventions and those identified through the IIUA activities along a concept of information integrity and emergency management. In the chart below, the categories with darker coloring had more numerous activities associated with that phase of emergency management and aspect of information integrity.

Figure 3. Heat Map of Interventions During Russia's War on Ukraine



Source: Authors' calculations.

Unsurprisingly, there were more efforts in Safety, specifically in the Response stage, which overwhelmingly are areas of focus for tech companies. As mentioned earlier, Accuracy was also well supported in the Prevention/Mitigation and Response stages of emergency preparedness, largely thanks to robust fact-checking efforts. And finally, in ensuring continued access to information, Preparedness and Consistency was focused mostly on underlying infrastructure enabling continued access to the internet for Ukrainians.

While not a comprehensive listing of all possible activities that might comprise an information integrity-based emergency management framework, the table below provides a starting point for how democratic governments might consider developing such an approach.

Table 1. Developing an Emergency Management Framework

	Prevention & Mitigation	Preparedness	Response	Recovery
Consistency *(Regularity or steady continuity of access to information)*	• Invest in cybersecurity measures. • Implement laws to support media freedom.	• Develop and support public-private partnership (PPP) plans for deploying back-up connectivity and enhanced cybersecurity. • Conduct tabletop exercises to develop menu of response options and test against info integrity values. • Create conditions and/or incentives ensuring consistent access to reliable information in crisis. • Establish and exercise processes and protocols for information sharing across stakeholders. • Establish and support a joint coordination mechanism with a core team of coordinators. • Develop alternative means for communication. • Procure and provide VPNs as necessary.	• Provide emergency funding for temporary communications infrastructure. • Create channels of communications with CSOs to provide training and technical support to recover from cybersecurity attacks.	• Rebuild infrastructure. • Work with platforms to review/rescind emergency content moderation measures. • Assess state of consistency in info ecosystem.
Reliability *(Sustainability of results regarding information)*	• Invest in local media, independent media, and media development organizations. • Implement policies fostering independent and transparent media. • Support creation and maintenance of public broadcasters with national coverage. • Engage in robust transparency reporting to build public trust.	• Establish rules for engaging with media that maintain journalistic independence. • Create a flexible funding mechanism to support independent media. Pre-identify and pre-negotiate contracts with high-capacity pass-throughs to expedite how funding is processed. • Support regular assessments measuring state of media based on existing frameworks. • Connect media development organizations with independent media to develop plans for collaborative responses. • Source and plan for delivery of protective equipment. • Create plans for back-up newsroom locations, and foster partnerships between allied public broadcasters and independent media.	• Provide independent journalists and newsrooms with protective equipment. • Conduct consistent and factual information-sharing through public broadcasters. • Establish short-term funding to help independent outlets relocate or rebuild and continue reporting.	• Fund independent media to assist its rebuilding after the crisis. • Offer additional incentives to assist recovery (like tax credits and training). • Measure changes in state of reliability in info ecosystem.

	Prevention & Mitigation	Preparedness	Response	Recovery
Accuracy *(Quality or state of information being correct or precise)*	• Implement fact-checking and pre-bunking initiatives. • Ongoing monitoring of information ecosystem. • Create cross-sector norms and standards for maintaining information integrity and addressing disinformation. • Coordinate with CSOs and international organizations to develop criteria and create lists of trusted information sources for tech companies and international donors, while keeping media pluralism in mind. • Increase responsibility of media/ digital content producing entities. Facilitate connections between government agencies, CSOs, and tech companies to enable efficient monitoring and takedowns of disinformation.	• Engage local fact-checking organizations in providing training for tracking disinformation. • Develop coordination plans across various accuracy initiatives. • Implement systems for shared disinformation documentation, building on existing initiatives. • Support regular assessments measuring state of accuracy in the information ecosystem. • Develop contingency and support plans for front-line workers monitoring disinformation. • Produce indexes of trustworthy sources of information.	• Conduct regular and rapid-response fact-checking to address uncertainties during crises.	• Train and fund efforts to measure, evaluate, and address the impacts of disinformation and countermeasures.
Fidelity *(Degree to which audiences understand information as originally intended by the producer/ sender)*	• Support media literacy across populations. • Run awareness campaigns to prepare people for disinformation. • Civic education to build trust in democratic processes and institutions. • Engage in deliberative democracy processes to build trust with citizens.	• Conduct regular baselines on audience perspectives. • Create communication channels to engage audiences.	• Conduct regular public briefings and maintain open channels with public.	• Conduct public forums to address narratives that surfaced during crises. • Measure changes in state of fidelity in info ecosystem.

	Prevention & Mitigation	Preparedness	Response	Recovery
Safety *(Condition of being protected from or unlikely to be at risk of danger, risk, or injury)*	• Support digital safety initiatives across population.	• Support evidence locker/collection initiatives and training programs for using them. • Develop shared criteria and definitions for the kinds of evidence that could be used to prosecute war propaganda. • Engage tech sector to understand policies, and connect civil society to establish communication channels and lists of accounts needing enhanced security. • Implement means for assessing state of safety in info ecosystem.	• Collect and store evidence; inform media and the International Criminal Court of abuses. • Report policy violations and abuse on platforms through established channels.	• Engage the ICC in preparing a case against war propaganda. • Assess impact of digital safety measures. • Provide counselling resources for stakeholders impacted by abuse.
Transparency *(Quality of work being done in an open way without secrets)*	• Create mechanisms for transparency in engaging with industry and civil society.	• Clarify policies during crises and the processes through which decisions are made when national security concerns conflict with transparency needs.	• Maintain open and honest channels of communication. • Provide regular updates on changes in government policies under circumstances of duress.	• Contract independent auditors to identify opportunities for improvement. • Provide public, in-depth reporting on how coordination was conducted during crisis.

What Would This Combined II-EM Framework Provide?

Many gaps and challenges PCIO observed while attempting to coordinate multistakeholder efforts to assist Ukraine could have been avoided if the efforts had been conducted within the parameters of a formalized emergency management plan guided by principles of information integrity. For example, had emergency management plans been in place, democratic governments wishing to support Ukraine would have known from the outset the range of interventions available to them to mobilize more quickly, or scale up with partner countries.

In the status quo, private sector actors are expected to prepare and adapt to crises on their own. The lack of communication between governments and private actors has been costly. During crises, private sector actors often have to expend significant time and resources to explain to governments what plans their companies have in place. Then, when governments have been unable to clearly convey what they needed, problems have developed from mismatched expectations or even harmful efforts by companies.[14] An emergency management framework helps overcome these gaps in communication. For less-prepared private actors, a framework reduces costs of having to develop response plans from scratch during crises. If resources are a limiting factor, civil society organizations conveying that information to governments earlier on gives governments the time to devise training or funding mechanisms to support private actors. Across the board, this improves transparency in communication and reduces reputational risks private actors would face from failing to meet expectations that had not been conveyed.

The following section reviews those gaps and presents five key lessons identified during the project, and the ways an emergency management framework can help address them:

Lesson 1: Define Success

Gap: *Success was ill-defined to guide stakeholders.* Stakeholders across government, civil society, and industry often reported there was no clear vision for why interventions were being made in the information environment or how they were prioritized, other than a desire to end the war and help Ukrainians. But shared goals are crucial for a response strategy because they motivate stakeholders to cooperate, assist with prioritization of resources and activities, and provide milestones for measuring progress and recovery.

Solution: *Information integrity can provide a definition of success for stakeholders.* The six criteria outlined in the above definition of information integrity (Consistency, Reliability, Accuracy, Fidelity, Safety, and Transparency) can provide objectives and guidelines for how

stakeholders should be intervening within the information environment in line with democratic values, as well as possible future indicators of success through enhanced measurements within each category.

Lesson 2: Enable Constructive Coordination

Gap: *Coordination and convening are not the same.* Too little coordination was the most common gap identified through the needs assessment. Stakeholders reported significant duplication of efforts, not knowing what other stakeholders were doing, whom to go to for help, or how to navigate other stakeholders' organizational culture. The needs assessments with network members revealed that the activities outlined in each government's response often focused on those led by that specific department without much awareness of those led by other departments or agencies. At the same time, subsequent assessments of seventy-four publicly disclosed interventions by G7 RRM member states revealed that on average, seven separate types of government departments or agencies have been taking action in the information environment in relation to Ukraine. Effective coordination in a crisis builds on dedicated, tested and adequately resourced processes and personnel who could be mobilized and applied to mitigate, counter, and/or recover in a timely and appropriate manner.

Solution: *An emergency management framework provides a means of constructive coordination between stakeholders.* During crises, the urge to do something encourages overenforcement and duplication of efforts. Emergency management provides a toolbox for resolving bureaucratic uncertainties and overlap, providing a constructive opportunity for stakeholders to collaborate that moves towards a structured approach to responding to crises. Effective coordination occurs on a learning curve, and emergency management planning provides a framework for identifying areas in which coordination capacity should be developed. Emergency management planning led by a government in coordination with its allies will produce mapping of stakeholders, available resources, and capacities; delineate roles and responsibilities; and identify gaps and how to address them ahead of crises in the information environment. A coordinated approach using an emergency management framework would dictate the need for identifying points of contact, and developing corresponding mechanisms and processes in each democratic government could mobilize and prepare for deployment around a shared aim. If done as part of a joint effort, emergency management planning can help reduce inefficiencies by identifying who handles which responses and at which stage of the emergency planning process they occur. This enables better connections between stakeholders while avoiding duplications and presents opportunities to align and scale up efforts where possible. It also creates space for those who feel left out of the process to identify areas they can contribute to. Formal adoption of an emergency management plan would also present opportunities for stakeholders to engage with broader publics in ways that foster greater societal resilience in a transparent manner. The inherent structure of an emergency management framework presents a clear and familiar focus for engagement, helping different stakeholders see how they fit in, and what is being asked of them upfront.

Figure 4. Publicly Disclosed Government Interventions Related to Ukraine Across G7 RRM Members

Source: Authors' calculations.

Lesson 3: Build Subject Matter Capacity

Gap: *Lack of capacity.* A lack of skills and expertise was another top gap emerging from the needs assessments. The areas were wide-ranging, and included training on measurement and evaluation, and monitoring and analyzing disinformation. Specific expertise gaps that arose were for international law experts to explore how war propaganda could be used as evidence in war crimes, to guide tech companies to better help civil society raise issues, to glean insights into how "evidence lockers" could be maintained by tech companies to support prosecutions, and to receive technical expertise to mitigate a variety of cyber risks. The analysis of various capacity gaps identified by stakeholders pointed to several issues requiring an in-depth study. While there are many capacity gaps identified, which of these belong to activities directly linked with providing an immediate response in a crisis? Which mitigate risks or support the preservation of an integral information environment in a democracy? These assessments and categorizations must be part of a comprehensive strategy (see Lesson #1), informing the government's subsequent budgetary and capacity development efforts.

Solution: *Capacity-building needs can be identified and prioritized using an emergency management framework.* Using this framework can help stakeholders identify gaps at different stages of emergency management and on criteria of information integrity, which can enable prioritization of capacity-building. Examples identified in the case of Ukraine included the need for secure, reliable back-up channels for communications and common standards for the measurement and evaluation of the Impacts of disinformation.

Lesson 4: Improve Funding Models

Gap: *Funding models fall short.* Failing to prepare for crises in the information environment becomes costly in the long term. Ukraine's independent media long struggled with getting sustainable funding and support for their work and has been further weakened by the war. Long-term funding strategies might bear few immediate results but are essential for the integrity of the information ecosystem. However, current funding models pose structural challenges to an integrated crisis response. Most donor programs are project-based, which creates a competitive environment among grant recipients that hinders the sharing of lessons between grantees. A lack of long-term funding encourages organizations to focus on short-term fundraising needs at the expense of long-term planning. Moreover, the needs during a crisis are urgent and require more flexible funding to support both existing and new initiatives. Needs change during a crisis, as was evidenced in the activities of Ukrainian media development organizations, which were initially able to repurpose existing grant support to sourcing and delivering protective equipment to independent journalists. At the same time, they no longer had the capacity to pursue new grant opportunities, and their alternative sources of funding through local services and training were lost due to the collapse of the economy. Funding models that work in peace are not necessarily fit for purpose in war. Under a strategic emergency management framework, it should be possible for governments and donors to pre-identify and pre-negotiate contracts with specific civil society partners with significant and relevant capacity and expertise who could be funded to practice their readiness, develop tools and materials, or spring into action on short notice. At the same time, a funding pool administered by an independent civil society partner or an international implementor could be used, under clear parameters, to support mitigation, response, and recovery activities on the ground.

Solution: *An information integrity-based emergency management framework can better inform funding needs.* Similar to meeting capacity-building gaps, using an information integrity-based emergency management framework can help donors better understand needs across all stages of responding to a crisis within the information environment, such that funding models can be revisited to provide different types of assistance based on needs. Such an approach could anticipate needs that would arise, for example, in shoring up independent media when a local economy is affected over a long period of time, or creating programs that can respond more nimbly or flexibly than existing granting programs allow.

Lesson 5: Incorporate Systems Thinking

Gap: *Systems thinking is needed to develop interventions for the information environment.* Given how stakeholders tend to operate within silos and on individual mandates, there is a lack of an articulated conceptual and practical framework to guide operations within the information environment. This experience demonstrated that without an overall framework, individual interventions by various stakeholders sometimes exacerbated confusion and distracted Ukrainian partners from actually pursuing activities with a more systemic outcome. Yet, any response in the information environment must necessarily be multistakeholder, given its role in the legitimacy of democracy. (For example, see the case study on prosecuting war propaganda.) The information environment is highly interconnected due to information and communications technologies (ICTs) but also the flow of people across borders. To that end, the conflict physically might have been isolated to Ukraine, but it quickly spilled across the region and into other countries within the information environment. Therefore, democracies need an approach that can account for multiple layers of geography and various stakeholder types, in particular those familiar with local cultures and languages, in developing a response to crises in the information environment.

Solution: *An emergency management approach enables systems thinking.* Stakeholders attempting to ensure the integrity of the information environment are often operating within silos. There are divides across stakeholder types—be that government, industry, civil society, or media. There are also divides across geographies, between those stakeholders within a country, or others in the wider region. Taking an emergency management approach helps stakeholders see the bigger picture and begin to respond within the information environment with greater awareness for the complex system that it is.

What Should Governments Do?

Building on experiences from Ukraine, the next step for democracies is to consider how to prepare for the next crisis that occurs. This would involve identifying what can be done to intervene in the information environment, following the framework as outlined above.

Develop an Information Integrity-based Emergency Management Framework

A key place for democracies to start coordination, with an aim toward developing a whole-of-society approach, is at home—namely, understanding the sum total of all interventions a government can make across departments and agencies.

In Ukraine, the Ministry of Culture's "Information Ramstein" iterates the need for a whole-of-society approach, acting as a public political initiative coordinating strategic approaches in countering Russian disinformation and building an international coalition to support Ukraine's efforts.[15]

To identify and develop similar efforts, democratic governments should map the range of options for intervention in the information environment across departments and agencies of each country, as well as available resources (financial, technological, human) to understand better what is collectively possible. Given the interconnectedness of the information environment, this should include responses that might happen both abroad and at home. This could include drafting voluntary roles and responsibilities for collaboration with partner countries vis-a-vis one another and external partners. With this plan in hand, a constructive dialogue with other stakeholders can begin with democracies soliciting feedback and inputs from external partners on what more can be done and how further forms of coordination can help. These conversations, in turn, can inform the development of a clear international framework with principles on how democratic governments should operate within the information environment, and what constitutes acceptable and unacceptable behavior. Thinking longer term to the implementation of a whole-of-society scaled emergency management framework, an independent intermediary might be required to account for power imbalances between stakeholders, namely that of government and industry vis-à-vis civil society. Such a body might also be responsible for drafting and maintaining an emergency management plan for crisis response in the information environment, convening stakeholders in so doing, and mediating between them when challenges arise.

About the Authors

Iryna Adam is a former research analyst in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. She is now a masters student at the Georgetown University Security Studies Program, where she focuses on emerging technology and disinformation. Previously, she worked on countering disinformation within international organizations and government agencies in Ukraine.

Samantha Lai is a senior research analyst with the Partnership for Countering Influence Operations at the Carnegie Endowment for International Peace. Prior to joining Carnegie, Lai was a research analyst at the Brookings Institution's Center for Technology Innovation and the Foreign Policy Research Institute. Her work has been featured by NPR, Lawfare, TechTank, and more. She holds a B.A. in Political Science from Wellesley College.

Arthur Nelson is deputy director of the Technology and International Affairs Program at the Carnegie Endowment for International Peace. He works on international security and governance issues in cyberspace and oversees the program's research development, strategic planning, and policy engagement.

Alicia Wanless is the director of the Partnership for Countering Influence Operations at the Carnegie Endowment for International Peace, which aims to foster evidence-based policy-making for the governance of the information environment. Alicia was a technical advisor to Aspen Institute's Commission on Information Disorder and is a founding member of its Global Cybersecurity Group. She is also an expert advisor to the World Economic Forum's Global Coalition for Digital Safety.

Kamya Yadav is a former research analyst in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. Kamya is now a PhD student at the University of California, Berkeley, where she researches gender, representation, and technology in the context of developmental political economy, with a regional focus on South Asia.

Acknowledgments

With thanks to Chris Beall, Matthew Graydon, and Theodora Skeadas for their contributions.

Notes

1 "G7 Leaders' Communiqué," Prime Minister of Canada, Justin Trudeau, June 28, 2022, https://www.pm.gc.ca/en/news/statements/2022/06/28/g7-leaders-communique/.

2 The information environment is the space where humans and, increasingly, machines process information to make sense of the world. This space consists of all the technology underlying the processing and distribution of information, enabling analogue, electric, and digital communications, including radio, television, social media, artificial intelligence, and gaming platforms. A key component of the information environment includes information in all its forms, from the spoken and written word to images and videos. The information environment is a complex and adaptive domain whose integrity is vital to the legitimacy of democracies due to citizens' agency over decisionmaking in elections.

3 Alicia Wanless, "The More Things Change: Understanding Conflict in the Information Environment Through Information Ecology," PhD diss. (King's College London, 2023), https://kclpure.kcl.ac.uk/portal/files/205036820/2023_Wanless_Alicia_1867483_ethesis.pdf.

4 Darwin Marcelo, Aditi Raina and Stuti Rawat, "Disaster Recovery Guidance Series: Private Sector Participation in Disaster Recovery and Mitigation," World Bank's Global Facility for Disaster Reduction and Recovery, 2020, https://www.gfdrr.org/sites/default/files/publication/Private_Sector_Guidance_Note_DRAFT%206_LOWRES.pdf; Pamela Falk, "World is facing the highest number of violent conflicts since World War II, UN chief says," *CBS News*, March 30, 2022, https://www.cbsnews.com/news/most-violent-conflicts-since-world-war-ii-un-says/; "Global Protest Tracker," Carnegie Endowment for International Peace, accessed June 28, 2023, https://carnegieendowment.org/publications/interactive/protest-tracker; Zach Rosson, Felicia Anthonio and Carolyn Tackett, "Weapons of Control, Shields of Impunity: Internet shutdowns in 2022," Access Now, February 2023, https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf.

5 "Digital Responses to Crises: An Action Plan for Platforms and CSOs Confronting Online Threats," National Democratic Institute, October 18, 2023, https://www.ndi.org/publications/digital-responses-crises-action-plan-platforms-and-csos-confronting-online-threats.

6 Paul M. Taylor, "Article 20: Propaganda for War and Hate Speech," In *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights*, 579–90, Cambridge: Cambridge University Press, 2020, doi:10.1017/9781108689458.023.

7 Tim Bernard, "Inside the White House Roadmap for Information Integrity Research," Tech Policy Press, January 31, 2023, https://techpolicy.press/inside-the-white-house-roadmap-for-information-integrity-research/; Niamh Hanafin, "Strategic Guidance: Information Integrity: Forging a pathway to Truth, Resilience and Trust," United Nations Development Programme, February 16, 2022, https://www.undp.org/policy-centre/oslo/publications/strategic-guidance-information-integrity-forging-pathway-truth-resilience-and-trust.

8 OECD, forthcoming, "Tackling Disinformation: Strengthening Democracy through Information Integrity," OECD Publishing, Paris.

9 "Emergency Management Definition, Vision, Missions, Principles," Federal Emergency Management Agency, last accessed June 5, 2023, https://training.fema.gov/hiedu/docs/emprinciples/0907_176%20em%20principles12x18v2f%20johnson%20(w-o%20draft).pdf; Enrico Louis Quarantelli, "Emergencies, disasters and catastrophes are different phenomena," University of Delaware Disaster Research Center, 2000, https://udspace.udel.edu/server/api/core/bitstreams/7f8df691-a569-4374-bf43-a0c6b36c392c/content.

10 *An Emergency Management Framework for Canada - Third Edition,* (Canada: Public Safety Canada, Ministers Responsible for Emergency Management, 2017), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-en.aspx.

11 "Whole-of-Society Pandemic Readiness - World Health Organization," World Health Organization, accessed June 26, 2023, https://cdn.who.int/media/docs/default-source/inaugural-who-partners-forum/2009-0808_wos_pandemic_readiness_final7e244f53-ec76-420d-836e-758c25e2ddf5.pdf.

12 "Guide for All-Hazard Emergency Operations Planning," U.S. FEMA, September 1996, https://www.fema.gov/pdf/plan/slg101.pdf; "All-Hazards Risk Assessment," Public Safety Canada, September 19, 2023, https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-ssssmnt-en.aspx.

13 Mikael Wigell, Harri Mikkola, Tapio Juntunen, "Best Practices in the whole-of-society approach in countering hybrid threats," European Parliament, May 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf; "Countering disinformation and building societal resilience," European Union External Action Service, March 16, 2022, https://www.eeas.europa.eu/eeas/countering-disinformation-and-building-societal-resilience_en; Jungwirth Rainer, Hanna Smith, Etienne Wilkomm, Jukka Savolainen, Marina Alonso Villota, Maxime Lebrun, Aleksi Aho, and Georgios Gainnopoulos, *Hybrid Threats: A Comprehensive Resilience Ecosystem*, (Luxembourg: Publications Office of the European Union, 2023) doi:10.2760/37899,JRC129019, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf. Flaminia Ortenzi, Robert Marten, Nicole B Valentine, Aku Kwamie, Kumanan Rasanathan, "Whole of government and whole of society approaches: call for further research to improve population health and health equity," *BMJ Global Health* 7, no. 7 (202), http://dx.doi.org/10.1136/bmjgh-2022-009972.

14 Lora Kolodny and Amanda Macias, "Senators ask Pentagon for answers on SpaceX's Starlink service in Ukraine," CNBC News, September 15, 2023, https://www.cnbc.com/2023/09/15/spacex-starlink-service-in-ukraine-subject-of-senate-letter.html.

15 Oleksandr Tkachenko, "'Information Ramstein', Or How to Win the Information War," The New Voice of Ukraine, September 24, 2022, https://english.nv.ua/opinion/information-ramstein-or-how-to-win-the-information-war-opinion-50272248.html.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Partnership for Countering Influence Operations

Influence operations are a complex threat, and the community combating them—academics, social platforms, think tanks, governments—is broad. The goal of the Partnership for Countering Influence Operations (PCIO) is to foster evidence-based policymaking to counter threats in the information environment. Key roadblocks as found in our work include the lack of: transparency reporting to inform what data is available for research purposes; rules guiding how data can be shared with researchers and for what purposes; and an international mechanism for fostering research collaboration at-scale.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org