JANUARY 2026
IW PERSPECTIVE

Communicative Deterrence: A Theoretical Concept for Deterrence in the Information Environment

Dr. Rupinder (Tina) Mangat - Defence Scientist - Defence Research and Development Canada

The West finds itself in a war it did not want. It is a war it did not realize, until now, which had already broken out. … It is a war, at the time of writing, the West is losing.
— Johnson and Clack, The world information war: Western resilience, campaigning, and cognitive effects

The West is losing because the information revolution creates a "fragmented, networked enemy," and adversaries use the asymmetric advantages of the information environment (IE) to build networks that work to create fissures in democratic societies and weaken democratic states' political will and institutions, which can later advantage adversaries in conventional confrontations. In Simpson's words, "We misunderstand the conflicts we fight in." Adversarial information operations (AIO) help adversarial states close gaps in conventional military power by curtailing political will. As Sun Tzu says, "In war the victorious strategist only seeks battle after the victory has been won." Information warfare

The views expressed in this articles are those solely of the authors and do not reflect the policy or views of the Irregular Warfare Center, Department of War, or the U.S. Government.

can help replace the gap in firepower for near-peer competitors and allow those competitors to, in Sun Tzu's terms, win without fighting.

The asymmetric advantage in the IE is often applied against civilians. In the past few years, adversarial actors have worked to disrupt trust in democratic process through disinformation. Deterrence thus becomes as much about protecting civilians as much as it is about stopping adversaries. For information operations, "the 'centre of gravity' is… the civilian population, suggesting that deterrence should seek not only to influence the adversary's cost-gain calculus, but also that of one's own and foreign populations." Governments thus need to deter adversaries in the IE and work to protect the citizens and the state.

Communication enables AIO such as disinformation insofar as 'bad' information must be communicated to create effects. Communication also helps build resilience. Resilience against AIO can be a form of deterrence by denial in the IE. The theoretical concept of communicative deterrence captures this notion of resilience through communication as deterrence. Building on the Communication Theory of Resilience (CTR), communicative deterrence captures communication's role in deterrence in the IE.

Deterrence

Deterrence works by discouraging adversarial actors from causing harm. It usually follows two pathways—deterrence by punishment and deterrence by denial—pursued separately or simultaneously. Deterrence by punishment relies on the threat of retaliation. Deterrence by denial relies on projecting the idea to the adversaries that the benefit of their actions would be so limited that it would not be worth the cost. Adversaries' perception of limited gains gives them pause. Deterrence by denial is arguably deterrence through resilience because adversaries pause their actions when they expect insufficient disruption of their opponents' routines. Resilience turns deterrence by denial inwards by focusing on the state and domestic population. Over time, resilience can show adversaries that their disruptive actions lack impact and therefore value.

Resilience

Resilience is about being prepared for and dealing with disruptions and returning to 'normal' afterwards. In the security context, resilience is establishing "socio-technical systems with the dynamic ability to anticipate and respond proactively to potential threats by learning and adapting." Thus, resilience is about predicting adversarial actions and building systems that endure as well as proactive and ongoing adaptation and mitigation. Disruptions often affect complex systems. International and domestic social, political, economic, and technical systems interact, sometimes in unexpected ways with unpredictable effects. This complexity and uncertainty make deterrence difficult. Resilience is "a unique paradigm for managing predictable unpredictability" in a "complex risk and threat landscape where preventing threat is less successful than establishing coping mechanisms." Deterrence is supported by resilience, and if deterrence fails, resilience can help cope with the aftermath.

The IE

With ubiquitous connectivity and democratization of information acquisition, generation, and propagation, the IE has become all-encompassing. Unfortunately, this has made publics a target for adversaries. Disinformation is one type of civilian—or public-targeting IO that has proliferated and succeeded. The lack of accountability and relative untraceability make the IE even more attractive as a vector of influence. China wants to move to "a position of parity or supremacy, without recourse to traditional war … The enabling phenomenon … is information warfare." Russia has developed expertise in operating in unconventional information blind spots. The IE thus provides asymmetric advantage to adversaries in disrupting democracies.

Communication and Deterrence in the IE

The complexity of the IE grows exponentially: "Contemporary social technology means that we are witnessing something new: information pollution at a global scale; a complex web of motivations for creating, disseminating and consuming these 'polluted' messages; … and breakneck speeds of communication between trusted peers." The average individual cannot critically evaluate and consume information accordingly. Adversaries leverage this 'fog of information' to spread their ideology and sow chaos.

Communication is a foundational process in IO because information must be communicated to achieve effects. Adversarial influence has been analyzed in terms of intent, truth, legitimacy, source, and origin of communicating actor, but given the difficulty of tracking intent, origin, source, and sometimes legitimacy , deterring in the IE should understand the role of communication—as process and as message—in the IE.

United States Cyber Command commits to "persistent engagement" in cyberspace, recognizing that constant work is needed to manage cybersecurity as technologies, tactics, etc. evolve. Persistent engagement in the IE should similarly involve ongoing offensive and defensive efforts and resilience development. Communication can help strengthen population resilience. Because the public is a target, it should be part of the deterrence calculus, especially as public resilience becomes a deterrence capability.

Communication and Deterrence in the IE

According to the Communication Theory of Resilience (CTR), resilience develops through communication. Resilience develops as individuals and groups such as communities and organizations communicate about their emergent context: "Resilience operates as a process embedded or situated in everyday life at ordinary moments of loss as well as at extraordinary and profound disruptions … These events can provoke responses such as stress, anxiety, or trauma. The reactions can then be followed with coping and adapting, and ultimately perhaps thriving and transforming." Resilience is the negotiation of living through disruption. CTR focuses on how communication enables resilience, identifying five overlapping and non-linear foundational processes:

(1) crafting normalcy;
(2) foregrounding productive action and backgrounding negative feelings;
(3) affirming identity anchors;
(4) maintaining and using communication networks; and
(5) putting alternative logics to work.

Crafting normalcy involves the "active framing of circumstances and retelling stories for different stakeholders." The post-disruption normal emerges from communicating about past and present circumstances and imagined 'normal' futures. Foregrounding productive action and backgrounding negative feelings is about focusing on actions that create positive changes towards recovery. The aim is not to suppress negative emotions, but to try and channel emotional energy into empowering actions instead. Identity anchors are "discourses upon which individuals … rely when explaining who they are." Anchors allow people to hold on to important parts of their pre-disruption identity while negotiating a new normal. Putting alternative logics to work is about creatively interpreting and responding to circumstances, developing alternative ways to understand and develop a new normal. Developing, maintaining, and using communication networks means creating and leveraging systems that aid in recovery by developing and leveraging social capital through support and resource sharing. These five processes are "communicative interventions to foster resilience."

Communicative Deterrence

If communication enables disinformation and resilience, where resilience is also deterrence by denial, then communication can help deter adversaries in the IE. Communication can build resilience through communicating assurances and pathways to preparedness to the public. Communicative deterrence is the use of communication to build public resilience in the IE as a deterrent to AIO. Communication here refers to both the message itself and the actions of crafting and delivering messages and engaging with the public. Deterrence refers to deterrence by denial through resilience. Resilience, like strategies of deterrence by denial, is also "unconditional and always in place." As the targets of AIO i.e. the public become increasingly resilient, the return of investment for adversaries decreases to the point where operations yield limited or no results, which deters adversaries.

Communicative deterrence leverages CTR's five foundational processes to better understand deterrence in the IE. For communicative deterrence, crafting normalcy would focus on developing a framework that captures a path forward. Libicki provides an example of a narrative framework that could be used in the IE: "A narrative that says that cyberattacks on … a country's infrastructure are beneath notice is a very different narrative than one that elevates the importance of cyberattacks to the point that being the target of an attack can justify a kinetic response. The latter says that an attack has touched a nerve. A strategy of insouciance says the exact opposite." AIO may similarly be cast as an insignificant part of the new normal. Narratives would need to be communicated to the public, understanding that in the current IE, the narratives will spread farther than the intended audience rapidly. Further, communication is a participatory process, so governance entities will need to remain open to learning how publics engage with the narratives; how they understand, manipulate, and propagate them; what they question about the narrative and how; and so on. The narratives will need to remain agile. Iterations will likely be required to allow for the strategy and narratives to be updated and amended in response to the interactions with and feedback from

the public. Deterrence is dynamic, and the current IE increases that dynamism exponentially.

In communicative deterrence, foregrounding productive action and backgrounding negative feelings would focus on what actions can help recovery from disinformation and promote those. Negative emotions will arise inevitably, and they need not be ignored entirely, but rather they need to be channelled into positive action. Backgrounding is about "reframing of the situation linguistically and metaphorically to one of constrained hopefulness." Pathways for channelling negative emotions into positive actions will need to be devised and supported while simultaneously acknowledging the negative emotions.

Affirming identity anchors for communicative deterrence would focus on identity factors that are, for instance, part of the socio-cultural fabric of the state or popular among the public or both. The aim would be to ensure that the narratives encourage productive actions aligned with identity anchors. Such alignment can help stabilize identity even as it inevitably changes in the aftermath of a disruption.

Maintaining and using communication networks is critical for communicative deterrence because they represent trusted ways of information sharing. As trust in governments declines or remains low, such networks that include various governance sectors and other trusted entities can help develop more confidence in communication from certain sources. These networks also reach individuals and communities where they are and can relay their concerns back to the centre in a more impactful manner.

Communication networks can help parse emerging logics and weave them through the narratives being generated. Alternative local logics can also inform the central nodes of communication if particularly persistent logics emerge. For instance, Libicki's logics on understanding cyberattacks one that argues for a kinetic response, while the other takes an indifference approach—can be further nuanced through what emerges through the communication networks.

Conclusion

Communication is a factor for conventional deterrence, and this paper makes a case for communicative deterrence in the IE. AIOs are enabled through communication, so is resilience, and the latter works as deterrence by denial. Communicative deterrence can leverage communication as a resilience enabler to deter AIO. The five pillars of CTR have been adapted to communicative deterrence with the aim to establish CTR's five foundational processes as a way to develop resilience in the IE.

Dr. Rupinder (Tina) Mangat is a Defence Scientist with Defence Research and Development Canada. Her research is focused on the role communication plays in defence and security issues. Her current research interests include the information environment, adversarial information operations, and resilience and deterrence in the information environment. She has previously conducted research on strategic communication, diversity and inclusion in the military, the military's increasing role in domestic disaster relief, and climate change communication