

# CTX

## EDITORIAL STAFF

ELIZABETH SKINNER *Editor*  
ELIZABETH ROBINSON *Copy Editor*  
SALLY BAHO *Copy Editor*

## EDITORIAL REVIEW BOARD

VICTOR ASAL  
*University at Albany, SUNY*

CHRISTOPHER C. HARMON  
*Marine Corps University*

TROELS HENNINGSEN  
*Royal Danish Defence College*

PETER MCCABE  
*Joint Special Operations University*

RAJAN RAVINDRAN  
*Army Inidan, retired*

IAN RICE  
*US Army, retired*

ANNA SIMONS  
*US Naval Postgraduate School*

SHYAM TEKWANI  
*Asia-Pacific Center for  
Security Studies*

CRAIG WHITESIDE  
*US Naval War College*

Layout and Design provided by  
Graduate Education Advancement  
Center, Naval Postgraduate School

## From the Guest Editors

Today's global environment of strategic competition poses new challenges from adversaries seeking to disrupt the international order and further their anti-democratic influence at the expense of US, ally, and partner interests. While the threat of a conventionally fought international war has, so far, deterred actions that might trigger a major conflict, adversaries are conducting hybrid operations that are often not attributable and/or fall below the threshold of a traditional *casus belli*. The perceived success of previous hybrid campaigns—most prominently, Russia's incursions into Georgia in 2008, Ukraine in 2014, and now, Ukraine again in February 2022—has emboldened other adversarial powers such as China, Iran, and North Korea, along with several non-state actors, to seek to further their interests through aggressive hybrid activities.\*

NATO defines hybrid threats as a combination of “military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations.”<sup>1</sup> These threats are multi-domain (land, sea, air, space, and cyberspace) and often interdisciplinary. They are likely to be with us for the long term, and defeating them will require a comprehensive approach at many levels. While the United States and its allies and partner-nations have already taken steps to protect against and confront such complex challenges, there is still a great need to enable more effective responses, enhance deterrence, and increase shared awareness, understanding, and resilience.

The articles in this special issue of *CTX* address and analyze critical issues encompassing the nexus of hybrid threats and energy security. The goal is to share best practices and lessons learned in order to help the United States, its allies, and its partners develop and maintain a strong deterrence posture.

The issue begins with an article by Paul Mason Carpenter, Paul Sullivan, and Dan Nussbaum that discusses the importance of teaching military officers all aspects of operational energy (OE). OE, as the authors explain, is an indispensable attribute of military strength, has played a pivotal role in combat successes and failures throughout history, and powers almost all forms of communication and information-gathering and processing in the field. In today's energy-reliant

environment, officers need to understand what OE is, where it comes from, and how to use it efficiently and effectively for sustaining today's military forces and weapon systems.

The next article examines the NATO Coherent Resilience Tabletop Exercise program, which was developed by the NATO Energy Security Center of Excellence to enhance the resilience of allies and partners confronted with hybrid threats to energy infrastructure. Oleksandr Sukhodolia and Lawrence Walzer show how the tabletop exercise can be a useful tool to help regions and nations assess threats, identify response requirements, and develop potential solutions for countering hybrid threats.

In the third article, Adair Douglas, Alex Pina, and Meredith Pringle describe how Energy Resilience Tabletop Exercises (ERTTXs) and Energy Resilience Readiness Exercises (ERREs) can be used by military facility operators to prepare for, withstand, and recover from major electrical disruptions, whether the cause is natural or man-made, accidental, or deliberate. The authors describe how these exercises can identify gaps in planning, training, and preparedness, and help facilities to prioritize improvements.

Next, Brenda Shaffer analyzes the role of energy as a catalyst for the reignition of war between Armenia and Azerbaijan in 2020. She uses this conflict as a case study to illustrate how many combatants are making extensive use of hybrid warfare to target their opponents' domestic energy production and supply infrastructure. Dr. Shaffer emphasizes that the weaponization of energy infrastructure is likely to play a major role in modern hybrid warfare and thus warrants further study.

Our final feature article, by Lieutenant Colonel Jonas van Hooren, discusses the ways in which defense forces can integrate their special forces and their cyber assets to respond to hybrid conflicts that involve weapons and defenses in the cyber domain. He pays particular attention to the institutional aspects of cyber-SOF integration, including the need for leadership education and a clear understanding of the cultural frictions that can arise on both sides.

Finally, the Ethics and Insights column offers a lecture by Jeremy Davis on the ethics of cyber warfare. Speaking to a class at the US Naval Postgraduate School in 2020, Dr. Davis raises difficult questions about whether the increasing use of remote technologies in warfare leads to

growing complacency regarding the human costs of war, and engages in a lively discussion of these issues with his audience.

As our long-time readers know, *CTX* is always looking for quality contributions to the journal. If you have experience or have done research in the fields of irregular warfare and/or special operations that you think will be of value to your peers, write about it and send it to [CTXeditor@GlobalECCO.org](mailto:CTXeditor@GlobalECCO.org) for review. There are no deadlines for submission; once a piece is accepted, it will generally appear in one of the next two issues. For more information about *CTX* and the Global ECCO project, go to <https://nps.edu/web/ecco>. You can also follow *CTX* and Global ECCO on Facebook and LinkedIn. If you have questions, don't hesitate to contact the editor, Elizabeth Skinner, at [CTXeditor@GlobalECCO.org](mailto:CTXeditor@GlobalECCO.org).

Lawrence Walzer and Tahmina Karimova  
Energy Academic Group  
US Naval Postgraduate School



ENERGY ACADEMIC GROUP  
NAVAL POSTGRADUATE SCHOOL



The Energy Academic Group (EAG) provides energy-focused graduate education, research, and outreach at the US Naval Postgraduate School.

Learn more at [nps.edu/energy](https://nps.edu/energy)

\* The articles in this issue were completed before Russia's February invasion of Ukraine, and therefore do not reflect that crisis.

#### NOTES

1. "NATO's Response to Hybrid Threats," NATO, 16 March 2021: [https://www.nato.int/cps/en/natohq/topics\\_156338.htm](https://www.nato.int/cps/en/natohq/topics_156338.htm)