

CTK

Volume 12, No. 1 2022



SPECIAL ISSUE

Hybrid Threats and Energy Security

ISSN 2162-6421 (online)
Winter 2022

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.”¹ 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 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.

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

* 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

Inside

FROM THE GUEST EDITORS

Lawrence Walzer and Tahmina Karimova



06

Foreword

Michael Rühle,
North Atlantic Treaty Organization



34

Energy in Conflict: The Case of the 2020 Armenia-Azerbaijan War
Dr. Brenda Shaffer, US Naval Postgraduate School



08

Operational Energy: Essential Knowledge for Military Officers
Paul Mason Carpenter, US Department of Defense, Dr. Paul Sullivan, Johns Hopkins University, and Dr. Daniel Nussbaum, US Naval Postgraduate School



42

The Integration of Special Forces in Cyber Operations
LTC Jonas van Hooren, Netherlands Ministry of Defense



16

NATO Tabletop Exercises to Further Energy Resilience and Security: Ukraine as a Case Study
Dr. Oleksandr Sukhodolia, National Institute for Strategic Studies, Ukraine, and Lawrence M. Walzer, US Naval Postgraduate School



54

ETHICS AND INSIGHTS
The Ethics of AI in Warfare
Dr. Jeremy Davis, University of Florida



26

Exercise Roadmap for Resilience: Requirements, Results, and Resourcing
Adair Douglas, Alex Pina, and Meredith Pringle, Converge Strategies, LLC



65

PUBLICATION ANNOUNCEMENTS

About the Contributors

Colonel Paul Mason Carpenter, retired, manages energy innovation transition in the US Office of the Secretary of Defense (OSD). He holds master's degrees in public policy, political science, military art and science, and national security strategy, and was a PhD candidate in political science. Col. Carpenter has served in four conflicts, was decorated for combat heroism three times, commanded at the squadron and group levels, and served at the USAF Europe, Air Staff, Joint Staff. He taught military strategy, logistics, and energy at the Eisenhower School of National Security and Resource Strategy.

Adair Douglas is a senior associate at Converge Strategies, where she crafts expert policy concepts, advocacy strategies, and messaging in support of advanced energy markets and grid modernization initiatives. Ms. Douglas previously served as a Government Affairs Manager, leading external advocacy efforts and outreach programs with energy associations, electric industry stakeholders, and policymakers. She received her BA in political science from the Catholic University of America.

Dr. Jeremy Davis is a postdoctoral fellow at the University of Florida, and prior to that was a visiting assistant professor at West Point. His current research is in normative and applied ethics, particularly with regard to the use of artificial intelligence in policing, bioethics, the ethics of war, and the philosophy of death. Dr. Davis is also a consultant with Compass Ethics, which advises clients on applied ethics in business and government. He earned his PhD from the University of Toronto in 2019 and a BA in philosophy from the University of Missouri.

Lieutenant Colonel Jonas van Hooren currently serves as a staff officer in the Netherlands Ministry of Defense.

Tahmina Karimova joined the US Naval Postgraduate School (NPS) in 2010 and the Energy Academic Group (EAG) in 2019. In 2021, she also began supporting the new Center on Combating Hybrid Threats. Prior to coming to NPS, she worked with various governmental and international organizations on issues of elections, gender equality, transportation, and telecommunications. She has earned MA degrees in intercultural communications and linguistics, public administration, and security studies. Her current research focuses on energy security, critical infrastructure resilience and defense, hybrid threats, international outreach, and partner capacity-building through research.

Dr. Daniel Nussbaum joined the Operations Research Department and the Engineering School at NPS in 2004, and teaches courses in Cost Estimating and Analysis. He has headed the EAG at NPS since 2013. He also provides cost estimating and business case analyses for major governmental organizations. Dr. Nussbaum has a BA in mathematics and economics from Columbia University, and a PhD in mathematics from Michigan State University. He did postdoctoral work in economics, operations research, and national security studies at Washington State University and Harvard University.

Alex Pina is a director at Converge Strategies, where he develops innovations for energy resilience, critical infrastructure, and clean energy. He previously served in the Massachusetts Institute of Technology (MIT) Lincoln Laboratory's Energy Systems Group, where he developed energy resilience exercises and assessment approaches that are now required throughout the US Department of Defense. Before joining MIT, he founded and led a solar energy company. Mr. Pina holds a BS in aerospace engineering and an MS in engineering and management from MIT.

Meredith Pringle is a director at Converge Strategies. Before joining Converge Strategies, she served as a project manager for the US Air Force Office of Energy Assurance, leading resilience-focused projects across the Air Force. Ms. Pringle previously worked in the Office of the Deputy Assistant Secretary of Defense for Installation Energy, supporting OSD energy resilience efforts and leading the congressionally mandated Annual Energy Management Report.

Michael Rühle is head of the Hybrid Challenges and Energy Security Section in NATO's Emerging Security Challenges Division, and is the lead developer of NATO's emerging climate-change agenda. Previously he was head of speechwriting in NATO's Political Affairs Division, and senior political advisor in the NATO Secretary General's Policy Planning Unit. Before joining NATO in 1991, Mr. Rühle worked at the Konrad Adenauer Foundation in Germany and was a Visiting Fellow at the Center for Strategic and International Studies in Washington, DC. Mr. Rühle has published over 300 articles and book chapters on transatlantic security issues, and co-authored a book on missile defense.

Dr. Brenda Shaffer is a research faculty member with the EAG at NPS. Her research focuses on the interplay between natural gas trade and foreign policy, and politics and energy in the South Caucasus, Iran, and the Eastern Mediterranean. She is a senior advisor for energy at the Foundation for Defense of Democracies and a senior fellow at the Atlantic Council's Global Energy Center. Dr. Shaffer is the author of several books, including *Energy Politics* (Philadelphia: University of Pennsylvania Press, 2009); she also edited, with Taleh Ziyadov, *Beyond the Resource Curse* (Philadelphia: University of Pennsylvania Press, 2012).

Dr. Oleksandr Sukhodolia is head of the Energy Security and Technogenic Safety Department at the National Institute for Strategic Studies of Ukraine, where his research focuses on national and energy security, energy policy, energy markets, and critical energy infrastructure protection. From 2007 to 2011, he served as Deputy Head of the Energy Security Department in the Secretariat of Ukraine's National Security and Defense Council. Prior to that, he served as Head of Department and Deputy Head of the State Committee on Energy Conservation. Dr. Sukhodolia holds a PhD in electrical engineering and a Doctor of Public Administration degree.

Dr. Paul Sullivan teaches courses on Energy and Environmental Security at Johns Hopkins University. He also teaches in the Yale Alumni College and is associated with the Atlantic Council's Global Energy Center. He retired from the National Defense University, where he had taught for 22 years, in 2021. He received his BA from Brandeis University and earned his MA, MPhil, and PhD from Yale University. Dr. Sullivan is widely recognized for his expertise in energy, the energy-water-food nexus, environmental issues, the Middle East, and parts of Asia, the EU, and Africa.

Lawrence M. Walzer joined the NPS faculty in 2017 as a program manager for the EAG. In 2021, he helped establish NPS's Center for Combating Hybrid Threats. Mr. Walzer's research interests include hybrid threats, strategic competition, critical infrastructure defense, energy security, energy in conflict, operational energy, and regional energy security issues. Mr. Walzer retired as a lieutenant colonel after serving nearly 22 years in the United States Marine Corps. He received a BA in political science from Buffalo State College and an MS in business administration from Boston University, and is a 2007 distinguished graduate of NPS's National Security Affairs program.

COVER PHOTO

Aerial view of a fully operational oil tanker at sea to deliver oil to a terminal refinery. (Photo by Songphol Thesakit via Getty Images)

DISCLAIMER

This journal is not an official DoD publication. The views expressed or implied within are those of the contributors and do not necessarily reflect the views of any governmental or non-governmental organization or agency of the United States of America or any other country.

TERMS OF COPYRIGHT

Copyright © 2022 by the author(s), except where otherwise noted. The *Combating Terrorism Exchange* journal (CTX) is a peer-reviewed, quarterly journal available free of charge to individuals and institutions. Copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research, or educational purposes free of charge and without permission, except if otherwise noted. Any commercial use of CTX or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published herein rests with the author(s) of the article, unless otherwise noted.

Foreword

*Michael Rühle,
North Atlantic Treaty Organization*

RUSSIA

UKRAINE

THE ONGOING CRISIS BETWEEN UKRAINE AND Russia offers some important energy security lessons. For example, when it comes to energy, geography is still destiny, and control of pipelines still confers both economic and political power.¹ The struggle between Moscow and Kyiv over the price of gas and the future of Ukraine's role in the transit of Russian gas to Europe is more instructive in this regard than a thousand economics textbooks.²

The Ukraine crisis is also a reminder that energy security is an integral part of national security, that depending for energy supplies on authoritarian states such as Russia can be a strategic liability, and that interdependence between the producer and the consumer is a chimera if the producer can go longer without revenue than the customer can go without gas (or vice versa).

But there is more. To destabilize Ukraine, Russia has applied a combination of military, semi-military, and strategic communication tools. Through the expropriation of Ukrainian energy assets and increased pressure on gas prices, Russia has also managed to integrate energy security into this strategy. These actions make it very clear that ensuring energy security today must include a thorough understanding of hybrid threats.

In the cyber era, the means of aggression and disruption have become even more indirect and stealthy than in the past; cyberattacks, hybrid warfare, and disinformation campaigns

have moved the threats to energy infrastructure to a new level. The scenario of terrorists on speedboats loaded with explosives trying to attack an oil rig should never be dismissed as obsolete, and using drone swarms to attack refineries remains a plausible threat. But the rapid diffusion of advanced technology means that even small terrorist groups, let alone hostile states, will be able to use invisible and often non-kinetic means to achieve their objectives.

Today's means of attack have become not only less visible, but also instantaneous. A cyber attack may offer little or no early warning. There will likely be no time for lengthy consultations or collective countermeasures. Nor is attribution of the attack to a specific perpetrator likely to be quick or legally perfect. This means that the defense has to be built into the very system that is liable to be attacked. Waiting for the cavalry is the wrong approach; the cavalry will almost surely arrive too late.

Hybrid threats against energy infrastructure are here to stay, because the transition from fossil fuels to renewable energy sources such as wind and solar will create new vulnerabilities. It is true that for many states the shift toward renewables will improve energy security by reducing dependence on oil and gas imports, which are vulnerable to geopolitical influence, pipeline disruptions, and even coercion. However, because renewables like wind and solar power are not available around the clock, they depend on sophisticated industrial control systems and distribution networks, as

well as advanced energy storage solutions. These systems are all vulnerable to cyberattacks.

What does all this mean? It means, first and foremost, that the security of critical energy infrastructure requires more than deterrence or defense. The fitting paradigm is *resilience*. Resilience shifts the defender's focus onto the very object that needs to be defended, rather than leaving it on the means of deterrence or, if deterrence fails, retribution. Resilient energy infrastructure may even have some deterrent value in itself: why attack if the attack is not likely to have the disruptive effect that the attacker is seeking? Even if "deterrence by resilience" may sound far-fetched to some, resilience is bound to become a major security paradigm.

Second, the exchange of best practices must reflect the new threat landscape. Concretely, this means that Critical Energy Infrastructure Protection can no longer be discussed without giving the cyber and hybrid dimensions their rightful place in the planning process. Visible armed forces doing visible things are only one piece of the puzzle—and perhaps even the less important piece. It is the invisible stuff that matters. NATO's partner countries play an important role in this exchange. For example, Ukraine and Georgia can offer valuable experience on Russia's hybrid tactics, including those used against energy networks. Allies and partners also need to share their experiences regarding new legislative tools they enact to counter hybrid actors, such as prohibiting entities of certain countries from buying national energy infrastructure. Over time, this sharing should lead to a repository of experience that will help countries meet and mitigate hybrid threats.

Third, the military community needs to be better connected with academia and, above all, with the private sector. With most energy and cyber networks in private hands, it will be crucial to build "communities of trust" through public-private partnerships, in which different stakeholders can share confidential information on cyber attacks and other security concerns. Creating such new relationships will be challenging, because multinational business interests and collective security interests may sometimes prove to be irreconcilable. Still, the nature of hybrid threats makes the established compartmentalization of responsibilities between the public and private sectors appear increasingly anachronistic.

Finally, as a deteriorating international strategic environment forces the transatlantic community to look afresh at its own defense requirements, it also needs to take a closer look at how the energy/hybrid nexus could impact its collective defense. If, for example, the rapid deployment

of reinforcements to NATO's eastern borders has to be contemplated, the security of the energy infrastructure that is truly "critical," i.e., that enables the timely movement of forces, becomes paramount. Energy supply disruptions and critical energy infrastructure failures affect not only a country's economy, but also its ability to effectively organize its defense. Energy supply is therefore a tempting target in warfare, including hybrid warfare, and preparedness for energy-related incidents is part and parcel of a holistic approach to defense.

Hybrid activities against energy assets have become a constant feature of international competition. However, there is no law of nature that makes this unpleasant and dangerous situation inevitable or permanent. Most hybrid actors have a face and an address. They can be countered, punished, sometimes deterred, but they can also be engaged. Unity is key. If NATO's allies and partners stay united, refrain from hyping hybrid tactics into a miracle strategy, and learn how to get better at meeting threats in the "gray area," we can blunt the hybrid weapon even if we may never completely eradicate it.

ABOUT THE AUTHOR

Michael Rühle is Head of the Hybrid Challenges and Energy Security Section in NATO's Emerging Security Challenges Division.

NOTES

1. The views expressed are the author's own and do not reflect official policy of NATO or any government or governmental agency.
2. See Andrian Prokip, "A New Era of Gas Wars between Ukraine and Russia?" *Focus Ukraine* (blog), 23 November 2020: <https://www.wilsoncenter.org/blog-post/new-era-gas-wars-between-ukraine-and-russia>



Operational Energy: Essential Knowledge for Military Officers

*Paul Mason Carpenter,
US Department of Defense,
Dr. Paul Sullivan,
Johns Hopkins University,
and Dr. Daniel Nussbaum,
US Naval Postgraduate School*

The US Department of Defense (DoD) defines operational energy as “the energy required for training, moving, and sustaining military forces and weapons platforms for military operations.”¹ Operational energy is essential for almost all forms of combat; as such, “commanding it” will be critical to warfare in the future.

OPERATIONAL ENERGY (OE) CAN BE THOUGHT OF AS A foundation of national defense and an indispensable attribute of military strength. Therefore, military members of all ranks should be educated on every aspect of OE. Over the past 100 years, energy has evolved to power literally every military capability of consequence; since the beginning of World War I, OE has played a decisive role in all major conflicts. In the present day, OE powers almost all forms of communication and sensing; fuels all air, land, sea, and space platforms; energizes all electrical devices; and is itself becoming a primary direct-fire weapon.

Given the importance of OE in combat, it is consequently also an area for adversary forces to target. Access to energy is often considered a “vital national interest,” and has been a *casus belli*: a reason to go to war. Therefore, it is paramount that DoD comprehensively educate officers and enlisted service members about OE throughout their careers. It is important that military leaders understand OE needs and capabilities at the tactical, operational, and strategic levels of conflict. Officers should also realize how OE, in all of its forms within multi-domain warfare, is positioned, maneuvered, and exploited within any given battlespace. With these goals in mind, this paper will discuss why officers should be educated about OE, what they must know about OE at various points in their careers, and to what extent they need to be educated about the different aspects of OE.

Why Officers Should be Educated about Operational Energy

History is a wonderful educator and can help provide insight into the future. In conventional wars over the past century, OE has played a pivotal role in combat successes and failures alike. Beginning in World War I, for example, petroleum became critical for expanding motorized armies and air forces. At the end of the war, British Foreign Secretary Lord George Curzon declared that “the Allies were carried to victory on a flood of oil.”² A French senator similarly stated that “oil—the blood of the earth was the blood of victory.”³

Over the past century, operational energy has played a pivotal role in combat successes and failures alike.

OE powered World War II to an even greater extent, and became a focus for major military battles. At the beginning of the war, the majority of Germany’s oil supply came from Romanian oil fields, which made those fields primary targets for Allied air raids.⁴ Beginning in the spring of 1944, the Allies executed the “Oil Plan”—a bombing campaign that systematically targeted elements of German oil production such as oil fields, refineries, and plants that produced synthetic oil.⁵ Within months, the campaign had cut Germany’s output of petroleum, oil, and lubricant to less than ten percent of its previous levels, causing major shortages of fuel for the army’s mechanized divisions and the Luftwaffe’s pilot training program.⁶ Germany’s Minister for Armaments and War Production Albert Speer described the methodical attacks as “catastrophic” to the German war effort.⁷

Operational energy is an integral aspect of both the direct and indirect methods of warfare, and is a factor throughout all spectrums of conflict. Energy superiority is the ability to fully exploit one’s own energy capabilities while simultaneously preventing the adversary from doing the same. While the United States has enjoyed energy superiority in battle since World War I, the world is evolving, and US energy predominance is being challenged by nations like China. Based on historical conventional warfare, the victor dominates energy capability. Victory in the OE domain occurs when friendly forces have access to efficient, effective, and sustained production of combat power when and where it is required, while the enemy’s combat power production is disrupted, degraded, or destroyed. Attaining OE superiority, therefore, should be a primary goal of the US military. For this reason, we argue that every US military officer should be educated about OE.

Today, the US Secretary of Defense’s Operational Energy–Innovation office focuses on three primary areas of OE development: powering the force, electrifying the battlespace, and commanding energy.⁸ Powering the force involves generating and maneuvering OE to all fixed and mobile platforms, while simultaneously reducing vulnerability. Electrifying the battlespace means developing OE into more efficient, effective, and less vulnerable electrical power that can accommodate multiple power sources. No longer can the operations commander simply trust the logisticians to have fossil fuel in place when and where it is needed. In the future, OE decisions will be more complex and will require an immediate understanding of the battlespace before forces maneuver and expend OE. Commanding energy necessitates near-real time OE awareness, in order to exercise command and control (C2) at all levels of conflict—tactical, operational, and strategic. Therefore, it is imperative to require continuing OE education for officers.

The ways in which energy is used in battle, and the kinds of energy that are being used, have changed dramatically over the last fifty years. For example, nations are rapidly developing and beginning to field directed energy weapons, including railguns, lasers, particle beams, and microwave arms. It is likely that these weapons will dominate the battlespace within a few years. Future force concepts envision highly dispersed forces throughout large geographic regions, and these forces will require OE that is immediately available on demand. Without an abundance of ready, secure, and forward-based OE, we argue that future militaries will falter and fail.

Without an abundance of ready, secure, and forward-based OE, we argue that future militaries will falter and fail.

One of the most important reasons to run war games is to be able to estimate the material, personnel, and energy needed for an operation. Napoleon lost significant battles when he ran out of horse feed.⁹ Erwin Rommel lost battles in the North African desert when he ran out of fuel for his vehicles.¹⁰ If Napoleon and Rommel had run war energy games, these results might have been different. While the reality of combat and other operations often leads to surprises, an officer need not compound the risks by miscalculating energy needs.

Modern OE encompasses much more than positioning fuel. Warfighting OE is also about managing multiple types of energy sources (e.g., petroleum, solar, hydrogen, nuclear fuel), generation (e.g., generators, convertors,

reactors), distribution (e.g., electrical wires, power beaming), and storage (e.g., batteries, convertors, storage tanks). Warfighting OE includes batteries, weapons (e.g., energy weapons, battery-powered missiles and bombs), weapon platforms (e.g., tanks, planes, ships, satellites), forward-based microgrids, and cyber/communication systems—all the aspects required to accomplish military missions throughout various warfighting domains. Many of the petroleum motors in weapon systems will be replaced by hybrids, and eventually by fully electrical/alternate-fuel engines that are charged from wireless support systems.

OE must be capable of powering deployed platforms and weapon systems that are dispersed to forward operating locations and are thus more vulnerable to enemy attack. Command and control of warfighting OE therefore requires understanding the energy status across the battlespace and directing adjustments, sometimes very quickly. Officers must know how to integrate OE planning and execution at all levels of war, maintaining a near-real time understanding and command of OE throughout all aspects of the battlespace. Officers must ensure that they know how and where to obtain the OE battlespace knowledge they need, so that they can contribute to the effort to develop more advanced OE capabilities.

A focus on OE education and training will have a major impact on OE development, budget, and operations; it will save lives and help to ensure mission success. DoD is the largest single consumer of energy in the world, and about 85 percent of the fuel used by DoD is for OE applications. In regard to combat, one in eight casualties in the Afghan and Iraq Wars happened during fuel movements. If officers of all ranks are trained to understand how OE systems operate, missions might be accomplished with greater safety and efficiency while using less energy or using non-petroleum sources.¹¹

What Officers Must Know About Operational Energy

What do our officers need to know? To begin with, they need to have a foundational understanding of the past, present, and potential future energy resources used in military activities and operations. Officers need to understand the technologies and supply chains, how to think about present and future energy supplies and uses, and how all of these can impact combat operations.

There are many ways to generate electricity, including solar photovoltaics, concentrated solar power, spaced-based solar, wind power, tidal and wave power, biomass, geothermal,

Energy Concepts

It is important for military officers and civilian specialists in defense science and technology, and in acquisition and sustainment to study the energy ontology, because it provides a framework for understanding the energy process and supply chain. The following is a partial glossary of important energy concepts:

Sources: basic elements that “contain” energy (petroleum, coal, sunlight, etc.)

Power Generation/Conversion: converting sources to useable energy

Transmission/Distribution: making energy available to users

Storage: methods to store energy for later use

Energy Management: awareness, command, and control of energy

Tools and Analytics: methods to improve current systems and develop new capabilities

Platforms: mobile vehicles of all domains (land vehicles, aircraft, ships, satellites, etc.)

Weaponry (specifically military): includes energy weapons

Education and Training: career-long learning for all military personnel

coal, natural gas, oil, and nuclear power, among others.¹² To run operations effectively, officers need to know how the various energy systems they rely on work, including their supply chains, and what needs to be done when systems fail or when the supply chain is interrupted. Some training in both large and small electricity grids, microgrids, and battery and storage systems will help all officers understand how these systems function, and how to restore essential electrical systems in times of conflict and war.

Markets and Supply Chains

Most ships, vehicles, and aircraft used by the US military are fueled by oil-based products. The volatility of prices for



petroleum and refined products creates its own set of risks. Therefore, an understanding of energy markets is vital for officers, especially those involved in logistics, planning, and intelligence. Such understanding will enable them both to estimate their budgets and needs, and to appreciate the risks involved with relying on specific markets for energy, energy storage, and more. Diversity of sources can be key to saving lives and mission success. By gaining a better understanding of energy markets, officers will better understand the impact of new technologies, new entrants into the markets, the competitive or contestable nature of the markets, energy substitutes and complements, and how energy markets may be interlinked. Furthermore, since much of the infrastructure required by solar, wind, and other renewable technologies typically comes from overseas suppliers, it is important for officers to understand how tariffs, quotas, trade disputes, and trade agreements may affect the military's ability to acquire those technologies affordably, reliably, sustainably, and on time.

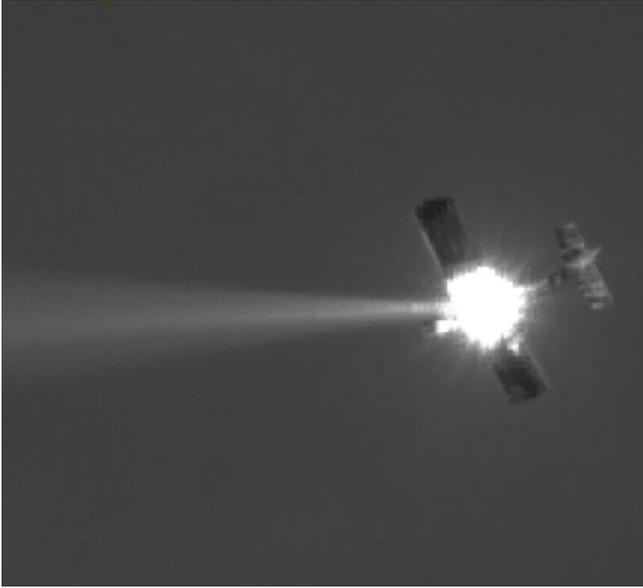
The supply chains for fuels are directly linked to electricity markets. The supply chains for natural gas and coal in the United States are mostly domestic. Global supply chains for fossil fuels, including coal, natural gas, and petroleum, often have important geopolitical ramifications. When fuel is needed for military activities outside of the home country, then a deep understanding of the local, regional, and global markets for the fuels and technologies that will be required in the area of operations is crucial, as well as an understanding of the rules that apply at each level. Oil markets are mostly global, but there may be local, regional, and national rules that can apply at times. Although natural gas

markets are usually regional, the distribution of natural gas is often local, with local rules and regulations that officers should understand.

A deep understanding of the local, regional, and global markets for the fuels and technologies that will be required in the area of operations is crucial.

Electricity markets can be some of the most regulated energy markets, usually under the control of public utility commissions or their equivalents. There are also, however, electricity markets that have been unbundled, so that generation, transmission, and distribution are the responsibility of separate entities. Understanding local electricity auction markets also helps with “hedging,” whenever that is allowed. In the context of this paper, hedging is defined as a way to acquire energy for distribution that minimizes customers' vulnerability to the high volatility of the wholesale energy market.

Even though each electricity market, whether domestic or abroad, has its own peculiarities, it is important for acquisition officers to understand what a market is, how markets behave (including during times of stress), how stable and controlled prices may remain over time, and the people with whom to communicate and negotiate. While the US Defense Logistics Agency (DLA) is currently the DoD agency charged with addressing many of these issues (petroleum acquisition, transportation, and storage) for the US military, senior leaders outside of DLA may be



The use of a high-energy laser aboard the Mobile Active Targeting Resource for Integrated Experiments (MATRIX) as it negates a UAS, 2010.

making strategic energy decisions in the future, as energy sources and energy generation become more diverse.

Transmission and distribution systems are different parts of the process of moving energy from where it is produced to where it is used. Electricity is sent from the generating source at a very high voltage over heavy transmission pylons and similar structures; it is stepped down in voltage when it transfers into a distribution system that carries it to its destination. Natural gas usually moves from a storage facility through high volume pipelines that cover long distances before connecting with the distribution pipelines that carry the gas to houses and other end users. Oil transmission pipelines known as trunk lines carry crude and refined products, including jet fuel, diesel, and gasoline, over long distances. These products are then distributed to various customers at various terminal points. Officers should be able to understand and map out these systems in the localities where forces are stationed, in order to identify potential points of failure and the places that may need extra protection. This information could be an important form of intelligence when planning an operation.

Energy Storage

Energy storage is an important aspect of supply chains that can have a direct effect on OE supplies. Energy storage comes in the form of batteries, pumped hydro, flywheels, chemical reactions, or heat storage (e.g., molten salts). Energy storage systems can be used for routine storage;

they can also be backup sources for vital and life-saving energy in times of stress when no other sources are available. Energy storage can tide over forward operating bases (FOBs) when fuel deliveries are interrupted, or when other methods of producing needed energy are not available. Without proper energy storage, energy systems could at times become unstable, or even unworkable. Determining the optimum way for soldiers and others to carry batteries and recharge them could mean the difference not only between victory and defeat, but also between life and death. Batteries and other storage options are also important for communications at all levels, from the individual to the battlefield. When an electricity grid goes down, an officer needs to know that there is a backup source of energy to tide the operation over until new supplies can be produced onsite or be transported in.

Platforms

Officers need to understand platform energy—the energy systems that are powering the ship, aircraft, or transport vehicle they are using. Miscalculations at the tactical and even strategic levels can happen, with the potential for mission failure in the near term, and service and national failure in the longer term. Lives can be lost due to such miscalculations.

Energy Weapons

As the energy weapons currently under development are fielded, they will pull heavily on the energy supplies of an operation. In some instances, they can be connected directly to platform energy: on an energy-integrated ship, for example, the energy used for such weapons will come from the same source as the power that runs the ship. Therefore, an officer on that ship needs to understand the tradeoff between having enough energy available to fire the directed weapon and to power and maneuver the ship.

Safety

Officers should also understand the safety issues related to fuels, electricity, and nuclear power, when these apply, and how to train their personnel in safe-use practices. For example, one of the hazards of high-voltage electricity systems is electric arc, when electricity jumps long distances. This can cause injury or death, and can damage platforms and other equipment. An officer dealing with the possibility of an electric arc needs to understand, at a minimum, proper grounding. Whether on an FOB, an aircraft, or a ship, the implementation of appropriate controls and procedures for handling power supplies is critical.

When preparing for any type of operation, whether on the battlefield or in training environments, officers need to know their energy requirements.

When preparing for any type of operation, whether on the battlefield or in training environments, officers need to know their energy requirements, energy use, energy safety issues, available energy storage, and the energy supply chains to sustain the operation. Energy must be an integral part of military C2, either as an independent system or as part of a comprehensive C2 system.

When to Educate Officers About Operational Energy

In recent years, DoD has begun to reinforce the importance of OE throughout the armed services. In 2012, Congress directed DoD to stand up an organization, Operational Energy Innovation, to manage the Operational Energy Capability Improvement Fund, which guides strategic and operational energy development and transformation across the services.¹³ In its *2016 Operational Energy Strategy*, DoD emphasized three objectives “to ensure the consistent delivery of energy to the warfighter:”¹⁴

- “Increase future warfighting capability by including energy as a factor throughout future force development.
- Identify and reduce logistical and operational risks from operational energy vulnerabilities.
- Enhance the mission effectiveness of the current force through updated equipment and improvements in training, exercises, and operations.”¹⁵

While implementation of these objectives requires the efforts of the Office of the Secretary of Defense, Defense Agencies, Joint Staff, combatant commands, and the military departments, the DoD must also use a holistic approach to education and training. Officers should be exposed to OE issues early in their careers and updated often, with a focus on information relevant to each officer’s rank and position. Officers must first be educated about OE at a tactical, introductory level. Then, as they progress through their careers, they will need to learn more operationally focused aspects of OE and, eventually, strategic OE, as it impacts the overarching planning and management of the forces.

It is very important that an officer understand the energy support that is available for operations and training. In the

United States, DLA-Energy is the major logistical support for DoD energy needs, working with the private sector and others to ensure there is enough energy available for DoD requirements. Officers need to know how DLA-Energy works and how to make use of its system; therefore, a visit with DLA-Energy should be required for all officers who are involved in the logistics and planning of major operations.

Given the importance of energy in operations, energy education should be part of the fitness reports for officers involved with energy logistics. These reports should also have markers for how well an officer plans, uses, and develops OE in his or her areas of responsibility.

Given the importance of energy in operations, energy education should be part of the fitness reports for officers involved with energy logistics.

Basic OE Education: Officer Training/Candidate School and the Service Academies

At the beginning of their careers, officers should begin to learn OE concepts and their impact on current tactical operations through Officer Candidate School or the service academies. OE education might be accomplished through an overview course that does the following: (1) introduces officers to the multi-disciplinary considerations of energy; (2) shows how mastering these OE issues provides strategic, operational, and tactical advantages over opponents; and (3) illustrates how failure to master OE presents an opportunity for enemy exploitation and friendly mission failure. The following key educational areas should be included:

- basic energy ontology and how it functions,
- energy superiority,
- energy sources and generation for tactical platforms and weapon systems,
- exploiting and maneuvering energy,
- basic OE resourcing and logistics.

Intermediate OE Education: Functional Career Courses and Intermediate Service Schools (ISS)

More tailored and detailed OE education should be integrated into the functional career courses (e.g., Supply Corps School) and ISS, particularly as it relates to operational warfare. Functional schools must teach about OE and its supply chains relevant to their areas of specialization. ISS

and senior military education schools offer a tremendous opportunity for OE education. Many of these programs take 10 months or longer to complete, and educate students in operational warfare and strategy. At this intermediate level, the following areas should be included:

- joint/coalition operational/theater OE planning and execution,
- operational C2 systems and OE components,
- wargaming and field exercising that includes OE,
- advanced near- to mid-term energy systems and how to operationalize them,
- adversary energy systems and how to interdict them.

Senior OE Education: Senior Service Academies

Flag officers and senior executive service candidates complete leadership courses upon selection. In addition, the vast majority attend a senior service school. As part of this education, these senior leaders should be introduced to the strategic-level aspects of OE and how these issues impact planning, operations, and management of the forces. Senior leaders need to have a solid understanding of the strengths, weaknesses, opportunities, and threats presented by OE, in order not only to command operational forces, but also to help advance military OE. Key energy areas that senior-level education should address include the following:

- national OE leadership and development,
- national energy resourcing and strategic stockpiles,
- future OE systems, economics, and funding,
- global energy C2 systems.

The military fights as it trains. Therefore, integrating realistic OE considerations and challenges into war games and tabletop exercises (TTXs) will provide critical education for officers at all levels. In fact, if realistic OE is not incorporated into war games and TTXs, officers' understanding of OE will be inadequate. Therefore, it is imperative that energy become a primary aspect of all military exercises, whenever possible and appropriate.

Conclusion

Energy education in DoD should take place across all levels and for the long term. As some enemies and competitors of the United States, including China, rapidly increase their use and understanding of OE, DoD needs to ensure that the US military can maintain its lead in OE development and deployment. In addition to educating all military personnel, it is important to develop a corps of “energy officers” who are constantly testing the energy pulse of their area of responsibilities, and who are also looking to the future energy challenges near and far. There is no place for complacency in a quickly changing OE world.

The military services use doctrine to establish baselines for education, training, and operations. However, the US military currently lacks a comprehensive energy doctrine;

It is imperative that energy become a primary aspect of all military exercises, whenever possible and appropriate.

the limited energy doctrine that does exist focuses solely on liquid fossil fuels.¹⁶ In future warfare, “strategic” OE will be optimized by doctrine, planning, and strategy. Thus, developing an overall energy doctrine is an important first step in the process of improving energy education for officers.

OE is a physical force, powering microgrids and platforms and functioning as a weapon itself. New and developing forms of warfare demand that energy be operationalized, with its full capabilities available from forward operating locations. Many weapon systems will likely evolve from their current engines to hybrids, and then to fully electrical engines that are charged from power-beaming systems. DoD is currently working with numerous universities and civilian labs to maximize efficiencies and take advantage of assets across the enterprise and research spectrum. Developments from DoD often spill over into the US civilian sectors, while the civilian sector supplies energy and technology for the DoD in turn. As a matter of total investment, the civilian industrial energy sector dwarfs that of DoD. Therefore, joint military/industry OE development and investment will be necessary in order for DoD to realize the best economies of scale. These are some of the many reasons why officers must be educated about OE early, often, and in ways that are relevant to their jobs throughout the course of their careers.

Sun Tzu noted that “in all fighting, the direct method may be used for joining battle, but indirect methods will be

needed in order to secure victory . . . these two in combination give rise to an endless series of maneuvers.”¹⁷ Today, OE is an integral aspect of both the direct and indirect methods of engagement and throughout all spectrums of conflict. Since the beginning of the twentieth century, the United States has had “energy superiority,” but this is being challenged today. Maintaining this superiority should be a primary goal of the US military, and educating officers in OE is an essential part of attaining that goal.

ABOUT THE AUTHORS

Paul Mason Carpenter is the Intake and Transition Chief for Operational Energy Innovation at the Office of the Undersecretary of Defense, US Department of Defense.

Dr. Paul Sullivan teaches energy and environmental security at Johns Hopkins University.

Dr. Daniel Nussbaum is the Chair of the Energy Academic Group at the US Naval Postgraduate School.

This is a work of the US federal government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

8. Paul Carpenter is a member of the Operational Energy—Innovation office and helped develop and implement the Secretary’s plan.
9. See Robert Burnham, “Why did Napoleon Fail in Russia in 1812?,” The Waterloo Association, n.d.: https://www.napoleon-series.org/faq/c_russia.html
10. See Niall Barr, “Rommel in the Desert,” BBC, 17 February 2011: https://www.bbc.co.uk/history/worldwars/wwtwo/rommel_desert_01.shtml
11. The information in this paragraph comes from the Office of the Secretary of Defense, Operational Energy Innovation Briefing, 15 December 2020.
12. With the proper safeguards, small modular reactors have considerable potential as a source of operational energy. Several countries are developing some version of these. See the International Atomic Energy Agency’s webpage on this topic for more information: <https://www.iaea.org/topics/small-modular-reactors>
13. “Operational Energy Capability Improvement Fund,” Department of Defense Research and Engineering Enterprise: <https://rt.cto.mil/ddre-rt/dd-rtl/oe-i/ocif/>
14. Department of Defense, *2016 Operational Energy Strategy* (Washington, DC: Office of the Assistant Secretary of Defense for Energy, Installations and Environment, Department of Defense, 2016), 6: <https://www.acq.osd.mil/eie/Downloads/OE/2016%20DoD%20Operational%20Energy%20Strategy%20WEBc.pdf>
15. Ibid., 6.
16. The only available Joint energy doctrine addresses petroleum fuels. The Services have incomplete energy doctrine.
17. Sun Tzu, *The Art of War*, trans. Lionel Giles (London: Luzac, 1910), chapter 5, verses 5 and 10: <https://suntzusaid.com/book/5>

NOTES

1. “Operational Energy,” Office of the Assistant Secretary of Defense for Sustainment: https://www.acq.osd.mil/eie/OE/OE_index.html
2. F. William Engdahl, *A Century of War: Anglo-American Oil Politics and the New World Order*, rev. ed. (London: Pluto Press, 2004), 39.
3. Yaw Yeboah, “The Lecture for The Prize Chapter 9: The Blood of Victory: WWI” (lecture for EGEE 120: Oil: International Evolution, Pennsylvania State University, University Park, PA, n.d.): <https://www.e-education.psu.edu/egEE120/node/233>
4. James Gadea, “‘Ulei Română’ During World War II and Beyond: Development of the Romanian Oil Industry,” *The Yale Review of International Studies*, October 2014: <http://yris.yira.org/essays/1474>
5. “WWII Allied ‘Oil Plan’ Devastates German POL Production,” Air University History Office, 26 June 2019: <https://www.maxwell.af.mil/News/Display/Article/1887774/wwii-allied-oil-plan-devastates-german-pol-production/>
6. Ibid.
7. Ibid.; RuthAnne Darling and Paul Mason Carpenter, “Energy: An Essential Element for Winning Future Wars—Operational Energy Part 1,” Surge (Fall 2020): 6: <https://nps.edu/web/eag/future-wars>

NATO Tabletop Exercises to Further Energy Resilience and Security: Ukraine as a Case Study

*Dr. Oleksandr Sukhodolia, National Institute for Strategic Studies, Ukraine, and
Lawrence M. Walzer, US Naval Postgraduate School*

FREEDOM, DEMOCRACY, AND SECURITY ARE threatened in many parts of the world by today's strategic competition and hybrid threats.^{1*} Critical infrastructure (CI), including electricity grids, transportation systems, water systems, and so on, is an essential component of modern societies' economic strength, security, governance, and way of life. To mitigate the challenges posed by hybrid threats to CI, many nations are seeking to enhance the resilience of their critical infrastructure protection (CIP) systems through a range of legislation and government action. To assist with these endeavors, NATO and its associated Centers of Excellence have highlighted the tabletop exercise (TTX) as a tool to identify areas of concern and bring forth potential solutions, while the NATO Energy Security Center of Excellence (ENSEC COE) developed the Coherent Resilience (CORE) TTX program to focus on CI and hybrid threats. This paper looks at the design, development, execution, and outcomes of the CORE program, with special emphasis on the TTXs conducted in Ukraine in 2017 (CORE 17) and late 2021 (CORE 20).²

Various nations and institutions have their own definition of the term "tabletop exercise." The US Department of Commerce's National Institute of Standards and Technology guide on training and exercises defines tabletop exercises as "discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation."³ This definition provides a useful understanding of the term as it is used in this paper.

The past several years have seen an increase in NATO exercises, many of which have also included partner countries. Thus, "following Russia's illegal 'annexation' of Crimea in March 2014, the number of exercises undertaken that year was increased and at their 2014 Summit in Wales, NATO leaders . . . have agreed on a strengthened deterrence and defence posture that draws upon all the tools at NATO's disposal, including military exercises."⁴

In Ukraine, a wider discussion of ways to adapt the national security system to hybrid threats resulted in the establishment of a program in December 2016 called the State System on CIP.⁵ While developing the CIP system, government agencies identified significant shortfalls in interagency cooperation, as well as the absence of a common working language and procedures for communication.⁶ A number of problems hamper the introduction of the CIP system in Ukraine,⁷ but the following are the most important:

- the need to shift government and public attention from a *reactive* policy focused on recovering from the consequences of a crisis to *preventing* crises by developing the capability to deter, mitigate, and more effectively respond to hybrid threats;
- the need to establish a system of coordination among CI stakeholders, including effective public-private partnerships, that will enable them to combine their efforts; and

* This article was completed before the February 24 invasion of Ukraine by Russia, and so does not reflect that crisis.

- the need to clearly define the function of a CIP system in order to ensure the continuity of essential services and the resilience of not only CI but the CIP systems themselves during crises.

To make progress toward improving CIP systems, officials must first have full awareness of the problems. This knowledge would help ensure that the necessary legislation is put in place to coordinate planning in the institutions that are responsible for the various system components' activities, such as intelligence, counterterrorism, civil protection, cyber security, physical protection, and so forth. Increased awareness would also lead the population to better understand the challenges they would face in crisis situations and their role in supporting efforts to protect and increase CI resilience. The training programs usually associated with security and crisis management operations, however, often lack broad, interdisciplinary attention to CI and the continuity of essential services during crises. Among the various educational training tools that are available, collective exercises such as TTXs are the most useful for developing a common understanding among participating institutions, particularly those that are accustomed to working according to their own specific procedures.

The training programs usually associated with security and crisis management operations often lack broad, interdisciplinary attention to critical infrastructure (CI).

The authors of this paper were directly involved in the design, development, and execution of a series of training events, in Ukraine and other Eastern Europe countries, that sought to highlight the objectives, structure, and challenges associated with conducting national-level TTXs on CIP.⁸ Exercise design, development, and execution is a detailed and lengthy process, and covering every aspect of the exercise planning for these training events is beyond the scope of this paper. With that in mind, this paper will discuss the TTX as a training tool, focusing on the key aspects of exercise design and execution, and will conclude by describing some of the results from the CORE TTXs in Ukraine.

Tabletop Exercise as Training Tool

Many nations' military, government, and CI stakeholders are not familiar with tabletop exercises. Even NATO's Bi-SC Collective Training and Exercise Directive 075-003 (referred to as Directive 075-003 hereafter) makes no mention of them. It does, however, provide a sound planning process for

exercise development, and serves as the primary source for NATO TTX planners, who will typically augment it with other NATO exercise directives, as well as doctrine from nations and organizations with detailed and formalized instructions related to TTXs.⁹ The US Federal Emergency Management Agency, for example, has a well-developed TTX training program and online reference materials that proved to be very useful for increasing the preparedness of organizations, institutions, and nations for crisis events.¹⁰

In general, there are several types of collective exercises for planners to choose from, depending on the purpose. They are either discussion-based or operations-based, and each has specific purposes, goals, and outcomes.

Discussion-Based Exercises

- **Seminar:** generally focused on enhancing understanding and a common framework within a group, which can be a starting point for developing or changing plans, policies, and procedures; seminars often lead to a product such as a report.
- **Workshop:** organized to develop a product or, at a minimum, to collect and/or share information through discussions, lectures, and facilitated breakout groups.
- **Tabletop Exercise:** intended to generate discussion and can be used to enhance general awareness, validate plans and procedures, facilitate conceptual understanding, identify strengths and areas for improvement, and/or influence the perceptions of participants.
- **Game:** developed as an analog or virtual simulation of operations in which participants' decisions and actions enable them to explore decision-making processes and consequences and evaluate existing and potential strategies.

Operations-Based Exercises

- **Drill:** a coordinated and supervised event to validate a specific function or capability in a single agency/organization, often used to validate a single operation; goals include practicing and maintaining skills, preparing for future exercises, and potentially evaluating new procedures, policies, and/or equipment.



Members of the Strategic Communications Syndicate discuss exercise inject responses during NATO Coherent Resilience 20 held during the Black Sea TTX in Odesa, Ukraine.

- **Functional exercise:** a simulation in a real-time environment that is designed to assess the capabilities and functions of primary components such as command posts and staffs.
- **Full-scale (live) exercise:** a time- and resource-intensive exercise, usually conducted in a real-time, stressful environment, that is intended to mirror an actual incident; the goals are to demonstrate participants' roles and responsibilities and the ability of multiple agencies to coordinate their responses.¹¹

A tabletop exercise was selected by NATO officials as the likely most effective method to facilitate Ukraine's efforts to develop greater CI resilience, given the current stage of its CIP system implementation. This is because the TTX is a low-risk, cost-effective tool that is designed to test and validate existing plans, policies, and procedures; highlight the capabilities of participating institutions; and identify resource requirements, capability gaps, strengths, areas for improvement, and potential best practices.¹²

TTX Design and Development

With the numerous resources available from national governments, organizations, agencies, and academic institutions, planners have a menu of options to support the design, development, and execution of TTXs. As mentioned earlier, the NATO planners who organized the CORE TTXs relied primarily on Directive 075-003, while also referring to other available sources as necessary and

appropriate. The exercise design established a multi-stage event according to the three stages outlined in Directive 075-003: (1) exercise concept and specification development; (2) exercise planning and product development; and (3) operational conduct and analysis, and reporting. The next sections discuss a few key elements within each of these stages in order to provide a general overview of the critical aspects of planning and conducting a TTX.

Aim and Objectives

When designing an exercise, it is important to incorporate objectives that will achieve the overall goals that senior leaders intend the exercise to accomplish. In general, a TTX's objectives should be in line with an aspect of the exercise nation's and/or institution's past, current, and future planning activities.¹³ If certain procedures are not yet defined in legislation or existing policies, the goal of the exercise may be to educate the participants about the specific challenges posed by certain threat or crisis scenarios, in order to identify any gaps that will require appropriate governmental or industry action to close. Objectives must be well-defined and achievable, and not leave participants feeling overwhelmed; such feelings can reduce active participation during the TTX.

In general, a TTX's objectives should be in line with an aspect of the exercise nation's and/or institution's past, current, and future planning activities.

The main purpose of CORE 17 was to involve Ukraine's government, industry, and nongovernmental organizations in meaningful discussions of how to respond to hybrid threats against critical infrastructure. The goal was to find gaps in existing crisis management plans, policies, and procedures, and to develop a consensus regarding what improvements needed to be made. Considering the status of Ukraine's CIP policy development and the exercise aims, these were the CORE 17 objectives:

- assess the resilience of CI and how well prepared the various system components were against hybrid threats (disinformation, cyber attacks, sabotage, covert operations);
- validate the effectiveness of national crisis management plans, policies, and procedures, including those that affect the energy supply, in their response to and ability to mitigate the effects and possible impacts of hostile hybrid actions;
- test existing measures to heighten the security of CI and supply chains, including those affecting military and civilian government institutions; and

- evaluate strategic communications procedures to mitigate the influence of malign hybrid actions, and to assess Ukraine's ability to coordinate with NATO members, partner nations, and international organizations.

These CORE TTX objectives reflected the needs of the different critical infrastructure sectors that ensure energy security and provide essential services.¹⁴ Every relevant organization was involved in the planning process, precisely to ensure that all equities were considered in order to create a highly realistic, useful, and challenging exercise.

TTX Planning

For each CORE TTX, planners identified three stages for the weeklong event: a two-day academic seminar with presentations and discussions to orient participants; a three-day scenario-based TTX; and a one-day "hot-wash" (after-action discussion) combined with a Distinguished Visitors Day. The CORE 17 events took place as follows:

Academic Seminar (Monday-Tuesday): This stage included presentations and discussions on the topics relevant to the planned TTX scenario, to orient participants and make them aware of the latest information regarding types of threats, best practices, and any recent changes in legislation. This preliminary stage of the exercise was developed to ensure that participants had the information they needed ahead of time and were prepared for the actual exercise.



Participants of the CORE TTX at the National Institute for Strategic Studies in Kyiv, 17 October 2017.

Tabletop Exercise (Wednesday-Thursday): The exercise gave participants the opportunity to increase their understanding of issues associated with CI resilience as they responded to threats to the systems at both the national and local levels. The exercise also encouraged governmental and private entities to coordinate their responses to simulated threats.

After-Action Hot-Wash (Friday): Stage three consisted of after-action briefings and a Distinguished Visitors Day. The briefings summarized the results of participants' discussions on the scenario responses and highlighted best practices, areas for improvement, and recommendations. The Distinguished Visitors Day was attended by senior leaders from the host country and NATO countries to discuss the initial TTX results.

The Training Audience

The target participant audience for the Ukraine CORE TTXs included middle- and senior-level personnel from the following: government agencies and ministries in the fields of infrastructure (e.g., transport, energy), economy and trade (e.g., sectoral industries), emergency services, national security and defense (e.g., Army, police, intelligence), local authorities, and CI operators. The main task in selecting trainees is to include personnel who are responsible for CIP and national resilience at both the national and local government levels; members of relevant nongovernmental organizations and institutions; operators of critical infrastructure; and members of industry associations, the media, and so on. As with all exercises, it is imperative that participants be the right people, from the right organizations, and in the right number.¹⁵

The main task in selecting trainees is to include personnel who are responsible for CIP and national resilience at both the national and local government levels.

Key Exercise Personnel

One of the most important factors of a successful exercise is skillful planning. Thus, the selection of key exercise personnel to fill the various roles in the TTX (exercise design, development, execution, and evaluation) is critical.

The following were some of the most important personnel roles for the CORE 17 TTX:

- **Exercise Planning/Control Team** developed and conducted the exercise, including the creation of a general plan for the training process, the exercise scenario, and all preparation materials and reference guides for facilitators and participants, and the coordination of training audience participation.
- **Participants/Players** responded to the exercise scenario based on their respective subject matter knowledge of current plans and procedures, and contributed insights to the discussions.
- **Observers/Subject Matter Experts** observed the exercise but did not participate in the discussions, except to provide answers to any technical questions that arose.
- **Co-Facilitators** were knowledgeable about and/or experienced in the subject material, and were responsible for keeping the discussions focused on exercise objectives. They also shared responsibilities for tracking time, announcing questions and injects (new events), following the discussion, and recording main findings and outcomes.
- **Evaluators/Data Collectors** gathered relevant information and ideas from the facilitated discussions during the exercise, so they could be incorporated into the final exercise report.

To ensure that everyone participates in the scenario-based discussions and that the allotted time is used most effectively, it is very important to have experienced and skilled facilitators. Some TTXs pair facilitators/moderators with assistant facilitators/moderators who play a secondary role, but we have found that having international experts and host-nation experts in co-equal roles is a better configuration for partnership exercises. At least one facilitator should be fluent in the host nation's language. Although they themselves do not participate directly in the discussions, facilitators must be able to both create an environment that encourages dialogue and guide discussions to prioritize key concerns and meet the objectives of the exercise. Because facilitators are often called upon to provide clarification on points of discussion, they need to understand the professional terminology related to the group's focus area, be experienced enough to make rational decisions, and be decisive enough to keep the discussion moving forward. Finally, facilitators must remain neutral and fair, and be comfortable with both allowing productive disagreements and ending fruitless debate if necessary.

Development of TTX Scenario and Exercise Events

Effective exercises are realistic and reflect current challenges confronting the exercise participants and organizations. For each CORE TTX, a Core Planning Team was designated and given responsibility for the development of the exercise scenario and corresponding events list—a series of vignettes and injects that are the basis for participant discussions.

The CORE 17 scenario was designed to reflect the kinds of real challenges to Ukrainian sovereignty posed by Russia in recent years.¹⁶ It is clear that Russia developed a deliberate hybrid war plan for its 2014 operations in Crimea, designed to achieve limited but specific objectives. The early phase included a multi-faceted influence campaign that sought to discredit the government of Ukraine. This was done to shape the battlespace and help ensure the success of subsequent kinetic hybrid operations that ultimately led to the achievement of Russia's main objective: the forcible annexation of Crimea.

Russia explicitly attacked Ukraine's CI in all phases of its Crimea operations in order to exert psychological pressure on the population.

Russia explicitly attacked Ukraine's CI in all phases of its Crimea operations in order to exert psychological pressure on the population and incite panic, social tension, and anger at the government; cause economic losses through the seizure of critical infrastructure and resources; and extensively weaken the government of Ukraine in the aftermath of the operation. It was in this context that CORE planners developed the TTX scenarios.

Each CORE TTX, all of which have focused on hybrid threats and energy security, has included significant elements of CIP. Using an "all-hazards" approach, the CORE 17 scenario and its injects comprised several different threats that would affect the continuity of services provided by CI.¹⁷ The base scenario reflected lessons identified and learned from studies of Russian hybrid operations launched against Ukraine since 2014.¹⁸

Each CORE TTX scenario has consisted of four to five separate stages, such as (1) pre-conflict phase: hybrid influencing; (2) low-intensity hybrid operations; (3) conflict phase: high-intensity hybrid operations; (4) hybrid warfare; and (5) post-crisis stabilization. These stages reflect what planners view as most realistic based

on the likely actions of the adversary and the necessity to "reset" after conflict subsides. CORE planning teams use the stages to identify sub-scenario vignettes and develop the corresponding event injects that will drive participant discussions. The vignettes describe the changing atmospherics that characterize each new stage in the exercise. A series of injects is then created for each vignette. For instance, an inject could be an explosion that takes place at a power generation facility and leaves the plant inoperable for several weeks. Participants would then discuss the likely effects of the power loss and the associated responses and obstacles. This is done for each inject that is presented.

To best accomplish the objectives of the CORE TTXs, participants are split into four or five "syndicates," each of which represents a different functional area. This format enables participants to focus their discussions on one specific area of concern according to the vignettes and injects.

Past syndicates have included:

- Strategic communications: focused on hostile propaganda and media manipulations as well as crisis communication;
- Site protection: related to cyber and terrorist attacks at the site, local, and national levels;
- Crisis response: concerned with energy-specific crises on the local and national level, and interagency interaction and information exchange; and
- International cooperation: working with allies, partners, international agencies, and nongovernmental organizations that may assist with crisis response and management at the international level.

The set of syndicates planned for each CORE TTX should reflect the exercise's objectives, so each TTX will likely have different syndicates. A brigade, for instance, could develop its own TTX with syndicates on command and control, operations, and logistics. Some exercises may not have any syndicates and instead keep all the participants in one group.¹⁹ Such considerations also come into play during the development of injects: some injects may be relevant to all of the exercise's syndicates, while others can be targeted for specific syndicates. The general concept of injects and syndicate interactions during scenario-based discussions is shown in figure 1. In a typical TTX, the entire training audience begins in a plenary session, where facilitators present a vignette and lead an interactive discussion about it among the audience members. The syndicates then move to separate work areas, where facilitators present injects

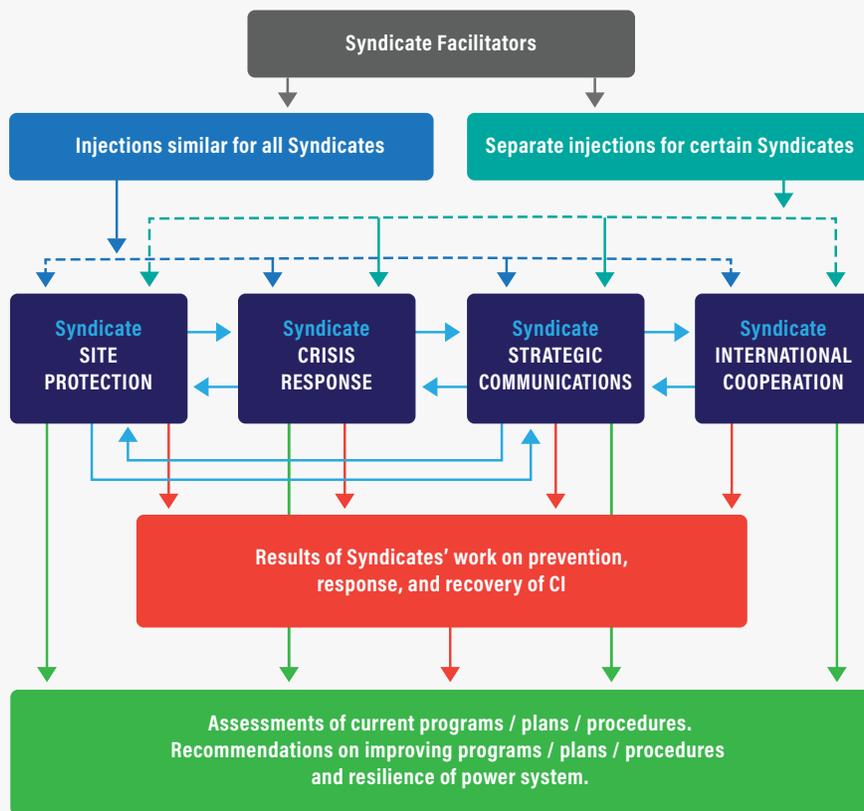


Figure 1: The General Concept of Injects and Syndicate Interactions²⁰

for the participants to consider. Each syndicate can choose how to prioritize and spend time on the different injects it is presented with, but all of the syndicates must complete their discussions concerning that particular vignette within an allotted amount of time. Once the time expires, the training audience regroup for the presentation of the next vignette, and so on.

During the “hot wash” debriefing on the last day, each syndicate presents its work so that the rest of the audience participants can interact and discuss the key takeaways. In more recent CORE TTXs, efforts have been made to increase syndicate interaction with tools such as chat rooms.

Conduct of a Discussion-Based TTX

The vignette-based discussion is the main aspect of a TTX, so it is imperative that these discussions be focused and guided to meet exercise objectives. Both facilitators and participants need to understand what the discussions are intended to accomplish and how they will take place. Therefore, facilitators may require some training before the exercise, as well as access to detailed preparation materials and tools.

As described above, the scenario, vignettes, and injects prepared for a TTX are designed to stimulate discussion and encourage participants to do the following things:

- analyze the vulnerabilities of their critical infrastructure, determine the consequences of a system failure, an attack, and/or damage to CI, and evaluate the possible consequences for other related dimensions of society;
- assess whether and how well the institutions, agencies, and organizations that provide crisis response and continuity of services cooperate and coordinate their work;
- exercise both civil and military crisis management processes and civil emergency planning in response to aggressive hybrid tactics at various phases of a developing crisis; and
- determine the gaps in plans and procedures and outline possible legislative improvements.

The CORE 17 TTX syndicates discussed their scenarios in three parts. First was a conversation surrounding the detection of an incident; second was the response portion of the discussion; and third, participants talked about the policy aspects based on areas identified for improvement. Each discussion followed a series of predetermined questions:

Discussion of detection: How does this case qualify as a security incident? What current mechanisms are in place to detect threats? How is the information verified? Who should be informed immediately? Who activates the procedures for responding to a security incident, and under what conditions? How might the identified threats affect CI? Which critical services or functions would be endangered in the case of a crisis? What might be the immediate and long-term consequences of damage to these aspects of CI?

Discussion of response: What could be done to mitigate or prevent negative consequences? What role, tasks, and areas of responsibility does each of the involved departments, agencies, or organizations have during the response? Again, who activates the procedures for responding to a security incident, and under what conditions? How does interaction between CI operators and local and national government bodies take place? Are there procedures for ensuring continuity of the functions and services provided by CI if it is damaged? Are there mechanisms for preparing the population for action in a crisis? How will the state and industry leadership, mass media, population, and international partners be notified and kept informed of events?

Discussion of policy: Could this situation be prevented? Are there any mechanisms for preventing the crisis from escalating? What are the procedures for responding to an emergency situation and how are they regulated by law? Is there legislation in place to establish or revise the requirements for the protection of CI facilities and objects? What aspects of prevention and response need to be improved?

Because high-level TTXs are not generally conducted on a regular basis, it is imperative that they are developed and executed in a manner that achieves the most comprehensive results possible.

Because high-level TTXs are not generally conducted on a regular basis, it is imperative that they are developed and executed in a manner that achieves the most comprehensive results possible. A detailed facilitators' guide, which is developed by the planning team and provided to facilitators ahead of the exercise, describes the exercise's goal, objectives, scenarios, vignettes, injects, and participating organizations. It also includes a series of discussion questions for the whole group and specific ones for individual syndicates or injects.

The TTX is not yet complete at the conclusion of the scenario-based discussions, of course. Now it moves to an analysis and reporting stage, which leads to the creation of a final exercise report.

The TTX Final Report

The reporting phase of an exercise aims to provide a full analysis and evaluation of the exercise against its stated aims and objectives. This report captures events as they occurred during the exercise, provides an analysis of the events relative to the exercise objectives, and suggests follow-on development actions to enhance or improve participating agencies' planning and response capabilities. This is done through the development of key takeaways (areas for improvement, strengths, and best practices) from the exercise and corresponding recommendations.²¹

The CORE TTX series relies on teams of experts to conduct the post-exercise analysis and prepare a report. The US Naval Postgraduate School's (NPS) Energy Academic Group has provided an evaluation team that has worked together with the CORE planning team, facilitators, and participants to capture the results of each CORE TTX and develop the findings into a final report. To ensure the report's accuracy and relevance, it is often necessary to partner with a host nation entity that is familiar with the country's legislation, plans, policies, and procedures. In the case of CORE 17 in Ukraine, the host nation partner for the evaluation was the Ukraine National Institute for Strategic Studies (NISS).

The final report covers all aspects of the TTX, but its main value is the presentation of the results of the TTX and the key takeaways. The report also has a section for each syndicate that summarizes every vignette and inject that was included in that syndicate's discussions, and presents

the syndicate's key takeaways. The conclusion features a section of overarching findings that are common to more than one syndicate's discussions and/or apply to broader areas of CIP than a specific syndicate's area of expertise. Interagency communications, for example, often show up in final reports as a challenge across syndicates.

The team approach to developing the final report leverages all the knowledge and experience of the professionals who take part in the exercise. For instance, the NISS personnel were experts on Ukrainian legislation; the facilitators were subject matter experts from several NATO nations with expertise on NATO best practices; and the NPS evaluation group incorporated US best practices where applicable. Finally, the training participants included senior

professionals with years of experience in hybrid threats and CIP, whose ideas to improve energy security systems and resilience are invaluable and need to be captured.

Conclusion

The CORE TTX has proven to be an effective tool to engage various state and civil institutions in the evaluation and assessment of existing capacities to meet modern CIP challenges. These exercises are also a useful way to increase government and industry leadership's awareness of the importance of contingency planning. TTXs help to build interagency networking, create trust among government institutions and other key stakeholders, and establish a common language that enables every actor to understand the threats to CI and the obstacles to resolving them.

These exercises are a useful way to increase government and industry leadership's awareness of the importance of contingency planning.

The CORE 17 and 20 exercises (conducted in 2017 and 2021, respectively) gave participants the opportunity to validate the policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations in the event of a threat or disaster. The controlled environment of the exercises allowed the participants to safely explore real-world solutions that would both improve response communication and coordination and advance the efficacy of broad-based public-private CIP partnerships. In addition, the CORE TTXs produced a range of practical recommendations aimed at improving Ukrainian state policy on CIP and crisis management plans.²²

Some of these recommendations have already been implemented through legislation. Soon after CORE 17, the Ukrainian government approved a resolution titled "The Concept for Building a State Critical Infrastructure Protection System in Ukraine," which outlines priorities for establishing a national CIP system and determines the main directions, mechanisms, and terms for the comprehensive legislative regulation of CIP activities.²³ The CORE 20 TTX was followed by President Volodymyr Zelenskyy's signature on a new law, "On Critical Infrastructure Protection," which serves as a roadmap to enhance the security architecture for CIP.²⁴

The Ukraine CORE TTXs included a broad list of participants from NATO allies, partner countries, and international agencies that participated in the International

Response syndicates. The goal was to review and assess the available means for international cooperation during crisis situations in a non-NATO country. Better coordination and cooperation between Ukraine and the international community in confronting Russia's aggressive hybrid operations have enhanced Western understanding of the adversary and deepened resolve to combat aggressive Russian activity throughout Europe and beyond.

Allies and partners seeking to improve national security and resilience against hybrid threats should consider implementing training and education programs that leverage TTXs as a means to identify areas for improvement, best practices, and potential solutions. There are several NATO entities that stand ready to provide assistance and expertise. Tabletop exercises, as demonstrated by the CORE program, are an invaluable means for allies and partners to further resilience and readiness to deter, deny, and defeat today's hybrid threats.

ABOUT THE AUTHORS

Dr. Oleksandr Sukhodolia is the head of Critical Infrastructure in the Energy Security and Technogenic Safety Department, Center for Security Studies, Ukrainian National Institute for Strategic Studies.

Lawrence M. Walzer is the deputy director of the Center for Combating Hybrid Threats, US Naval Postgraduate School.

This is a work of the US federal government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

NOTES

1. NATO identifies hybrid threats as combining "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. They aim to destabilise and undermine societies." "NATO's Response to Hybrid Threats: What are the Hybrid Threats NATO Faces?," NATO, 16 March 2021: https://www.nato.int/cps/en/natohq/topics_156338.htm
2. The CORE TTXs conducted in Ukraine in 2017 and 2021 were developed by the NATO ENSEC COE with the support of the NATO HQ Political Affairs and Security Policy Division (PASP), NATO HQ Emerging Security Challenges Division (ESC), and Cabinet Ministers of Ukraine. The NATO ENSEC COE has also executed CORE TTXs in the Baltic region and is in the process of planning two CORE TTXs in other regions.

3. Tim Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, National Institute of Standards and Technology Special Publication 800–84 (Washington, DC: Department of Commerce, 2006), 4-4: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf>
4. “NATO Exercises: Exercises Through Time,” NATO, 1 February 2022: https://www.nato.int/cps/en/natohq/topics_49285.htm
5. Decree of President of Ukraine No. 8/2017, “On Improvement of Measures to Ensure Protection of Critical Infrastructure Components” [in Ukrainian], 18 January 2017: <https://zakon.rada.gov.ua/laws/show/n0014525-16#Text>
6. Oleksandr Sukhodolia, ed., *Developing the Critical Infrastructure Protection System in Ukraine* (Kyiv: National Institute for Strategic Studies, 2017): 81–83.
7. Oleksandr Sukhodolia, “Implementation of the Concept of Critical Infrastructure Protection in Ukraine: Achievements and Challenges,” *Information & Security: An International Journal* 40, no. 2 (2018): 107-119: <https://doi.org/10.11610/isij.4008>
8. Oleksandr Sukhodolia, “Training as a Tool of Fostering CIP Concept Implementation: Results of a Table Top Exercise on Critical Energy Infrastructure Resilience,” *Information & Security: An International Journal* 40, no. 2 (2018): 120-128.: <https://infosec-journal.com/article/training-tool-fostering-cip-concept-implementation-results-table-top-exercise-critical>
9. NATO, *Bi-SC Collective Training and Exercise Directive (CT&ED)*, NATO Bi-SC Directive 75-3 (Norfolk, VA: NATO Supreme Allied Commander, Transformation, 2013): <https://www.act.nato.int/images/stories/structure/jft/bi-sc-75-3.pdf>
10. “National Preparedness,” Federal Emergency Management Agency, 21 December 2021: <https://www.fema.gov/emergency-managers/national-preparedness>
11. “Homeland Security Exercise and Evaluation Program (HSEEP)” (Washington, DC: Federal Emergency Management Agency, 2020), 2-6 – 2-11: <https://www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf>
12. Ibid.
13. Natasha Rotstein, “Designing, Conducting, and Evaluating Tabletop Exercises: A Primer on Optimizing this Important Planning Tool,” Center for Infectious Disease Research and Policy, 3 May 2007: <https://www.cidrap.umn.edu/news-perspective/2007/05/designing-conducting-and-evaluating-tabletop-exercises-primer-optimizing>
14. The CORE 17 exercise focused on critical energy infrastructure—specifically the national power grid—to facilitate contingency planning for the grid operator. CORE 20 focused on critical energy and transport infrastructure in the Black Sea region of Ukraine, with the goal to improve regional resilience against aggressive hybrid activity.
15. CORE 17 had more than 50 participants from Ukrainian ministries, agencies, and energy companies, in addition to 17 observers.
16. A vignette or scenario is “a sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses.” Grance, et al., *Guide to Test, Training, and Exercise Programs*, D-2.
17. An all-hazards approach is an integrated approach to emergency preparedness planning that focuses on capacities and capabilities that are required to meet a full spectrum of emergencies or disasters, including internal emergencies, a man-made emergency, or a natural disaster.
18. Vytautas Butrimas, Jaroslav Hajek, Oleksandr Sukhodolia, Dmytro Bobro, and Sergii Karasov, “Hybrid Warfare Against Critical Energy Infrastructure: The Case of Ukraine” (Vilnius, Lithuania: NATO Energy Security Centre of Excellence, 2020): <https://www.ensecce.org/data/public/uploads/2020/11/hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.pdf>
19. In comparison with CORE 17, for example, the CORE 20 scenario introduced an additional syndicate, MARSEC, which dealt with maritime security problems and freedom of shipping, and separated cyber operations and kinetic attacks into different syndicates.
20. Figure 1 was created by the author, from Sukhodolia, “Implementation of the Concept of Critical Infrastructure Protection.”
21. Vytytis Kopustinskas, R. Šikas, L. Walzer, B. Vamanu, M. Masera, J. Vainio, and R. Petkevičius, *Tabletop Exercise: Coherent Resilience 2019 (CORE 19)*, EUR 29872 EN (Luxembourg: Publications Office of the European Union, 2019): https://ensecce.org/data/public/uploads/2019/11/jrc118083_core_19_ttx_final_report_online.pdf
22. Sukhodolia, “Training as a Tool of Fostering CIP Concept Implementation.”
23. “On Approval of the Concept for Building a State Critical Infrastructure Protection System,” Resolution of the Cabinet of Ministers of Ukraine, No. 1009-r [In Ukrainian], 6 December 2017: <https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80>
24. “On Critical Infrastructure Protection,” Law of Ukraine No. 1882-IX (2021) [In Ukrainian], 16 November 2021: About critical infrastructure | from 16.11.2021 No 1882-IX (rada.gov.ua)

Exercise Roadmap for Resilience: Requirements, Results, and Resourcing

*Adair Douglas, Alex Pina, and Meredith Pringle,
Converge Strategies, LLC*

THE UNITED STATES EXPERIENCED 1.33 BILLION power outage hours in 2020, a 73 percent increase from about 770 million hours in 2019.¹ This increasing number of power outages impacts other infrastructure sectors and threatens the health of US citizens, and the nation's economy and security. The US Department of Defense (DoD) relies heavily on the nation's commercial electrical infrastructure to conduct critical missions, such as piloting remote aircraft, reviewing reconnaissance, and planning supply logistics from DoD facilities within the continental United States rather than from overseas bases. If a DoD installation doesn't have reliable electrical infrastructure, many of those missions could not be successfully executed. As natural disasters and determined adversaries threaten to destabilize the US electrical infrastructure, DoD must begin to think of *energy resilience* as a critical mission in and of itself.

This article explores how executing functional exercises can strengthen DoD's ability to prepare for, withstand, adapt to, and recover from installation or regional electrical disruptions. Using a hypothetical exercise scenario that illustrates the real-world challenges military installation energy managers face, the article describes how DoD has used Energy Resilience Tabletop Exercises (ERTTXs) and Black Start Exercises (BSXs) to test military installations' dependence on electrical infrastructure to execute critical missions, and highlights some of the ways in which the exercises enable DoD to support its infrastructure and mission success.

Not If, But When, We Lose Power

Imagine you are the energy manager at a military installation located on the West Coast of the United States. Your days have been filled with worry about recurring weather-related flooding that has taken place on and around the installation. In addition to the flooding, the installation is experiencing frequent blackouts due to high winds and



aging infrastructure. These blackouts have caused high-profile tenants to move from their buildings at the remote edges of the installation to contingency locations in the main cantonment. To add to the pressure, the installation is preparing for a satellite launch that has experienced multiple postponements. Leadership is anxious to get the launch accomplished.

Now imagine that, over the next 48 hours, you will learn that intentional tampering has caused a substation to catch on fire, regional power and wastewater treatment outages continue to impact the area due to the persistent flooding, and your utility provider has discovered that an adversary nation has executed a cyber attack on its distribution network.

Imagine that, over the next 48 hours, you will learn that intentional tampering has caused a substation to catch on fire.

No, this isn't a nightmare. This situation is an example of an energy resilience readiness tabletop exercise that was led by DASD(E&ER), the Deputy Assistant Secretary of Defense for Environment and Energy Resilience, at three DoD installations in 2019. Figure 1 provides an overview of the cascading sets of failures that could be used as the prompts for discussion during this ERTTX. The objective of testing high-stress scenarios like this is to prepare installation personnel for regional, prolonged electric power disruptions that would impact critical infrastructure, mission requirements, and personnel availability. DoD has prioritized the use of exercises that identify vulnerabilities in the energy capabilities of installation infrastructure that is directly related to critical mission requirements.

The exercise results have been used to support project development and prioritization across the US military. These exercises have primarily been either tabletop exercises or on-site energy resilience readiness exercises, also known as “pull-the-plugs” or “black starts”—live scenarios that begin with an installation losing its primary power source.

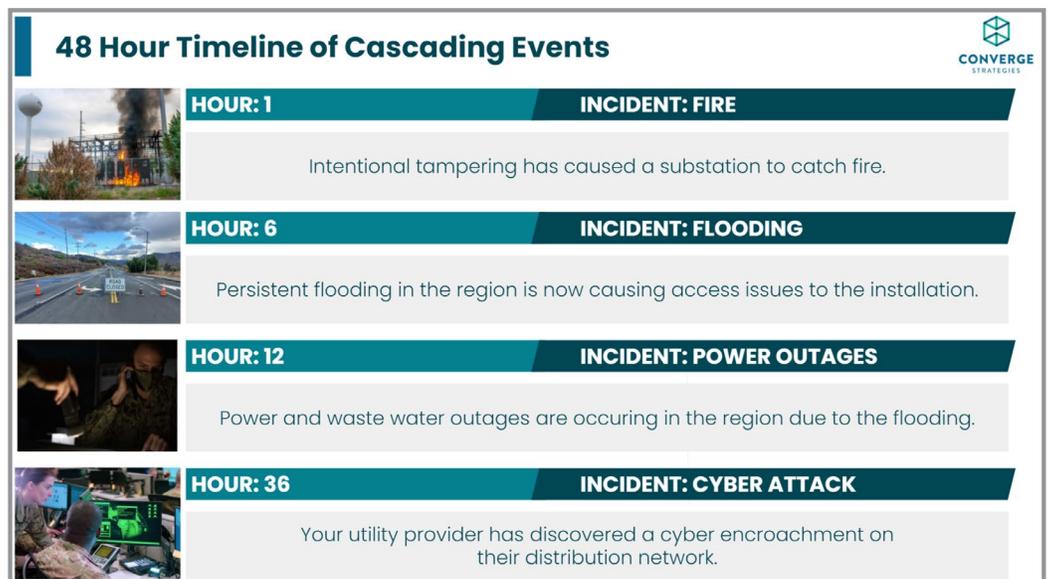
Figure 1. 48-Hour Timeline of Cascading Events²

The objective of an ERTTX is to scheme out how the installation would respond to events that test its ability to execute its missions. A subsequent BSX then builds on this scenario-driven plan by actually cutting off an installation's power for several hours to identify assumed and actual gaps between mission requirements, infrastructure, and personnel procedures. The following sections will discuss how, when, and why ERTTXs and BSXs should be executed, once the facility's requirements for energy resilience have been established.

DoD Energy Resilience

Energy resilience is defined for DoD as “the ability to avoid, prepare for, minimize, adapt to, and recover from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability sufficient to provide for mission assurance and readiness, including mission essential operations related to readiness, and to execute or rapidly establish mission essential requirements.”³ Vulnerabilities in the existing US electrical infrastructure are driving DoD's efforts to improve its facilities' energy resilience. US critical infrastructure is not only increasingly vulnerable to natural disasters, but is also facing a growing risk of cyber attacks by determined adversaries.⁴ As a result, energy resilience has been incorporated into several DoD policies over the last decade as a central tenet of mission readiness.⁵

In 2020, the US Government Accountability Office reported that more than 98 percent of DoD installations rely on commercial electrical infrastructure that exists “outside the fence line,” i.e., is separate from the installation. DoD's reliance on the commercial power grid requires a restoration and response plan that is shared across multiple



stakeholders, including the installation, utility providers, emergency responders, and community representatives. The Army, Air Force, and Navy have tracked the increasing severity and frequency of prolonged power outages and, in response, have mandated that their installations be able to sustain critical missions independent of the commercial electrical grid for a minimum number of days, ranging from seven days at Air Force bases to more than two weeks at Navy bases.⁶ There is, however, no general DoD requirement for the minimum number of days an installation will need to sustain mission operations if commercial power is not restored within those service-mandated timeframes.

Achieving Energy Resilience Through Exercises

Energy resilience exercises are an effective method that defense leadership can use to verify that installations are meeting their resilience goals.⁷ Recognizing the importance of integrating energy disruption scenarios into the military's exercise program to strengthen the energy resilience posture of DoD installations, DASD(E&ER) developed the ERTTX and BSX frameworks in 2018. It then executed three ERTTXs in which DoD installations faced hypothetical risk scenarios similar to those faced by the energy manager earlier in this article. Examinations of installation-specific infrastructure vulnerabilities, the region's history of natural disasters, and risks to the security posture of the installation helped inform the development of installation-specific scenarios that incorporated realistic threats to mission capabilities.

Energy resilience exercises are an effective method that defense leadership can use to verify that installations are meeting their resilience goals.

As of fiscal year 2021 (FY21), DoD had conducted more than 10 exercises using the ERTTX and BSX frameworks, and has dozens more exercises scheduled in the next five years. These exercises focus on creating a controlled, realistic environment that either replicates an adversary-caused power outage based on prior events, or builds on assessments of likely scenarios unique to the installation being tested. The exercises demonstrate the real-world gaps between critical mission requirements and infrastructure energy resilience, and give the installation personnel a unique opportunity to both practice their response to a grid power outage and validate the performance of the installation's systems, processes, and assets. The exercise results provide the installation with the proper justification

to request funding support for infrastructure improvements or to address critical gaps identified in the results.

The DASD(E&ER) exercises demonstrated their effectiveness in those initial programs; since then, the US Army, Navy, and Air Force have begun to develop exercise programs for their installation portfolios. In the FY21 National Defense Authorization Act, Congress required each US military service to conduct at least five "black start" exercises per year through FY27, "to evaluate the ability of the installation to perform critical missions without access to off-installation energy resources."⁸

Energy Resilience Tabletop Exercise

ERTTXs present participants with the scenario of a large-scale, multi-day event that would affect the commercial energy distribution system servicing a DoD installation. The participants then spend one or more days in a facilitated discussion of how they and their personnel would respond to the primary scenario and to each new input. The objective of the exercises is to test the ability of the installation's personnel to continue their mission during such an event, to demonstrate how the installation can support its mission through personnel response and infrastructure resilience, and to reveal critical gaps that need to be addressed. These gaps become the basis for planning resilience improvement projects that will enhance DoD's mission-readiness posture.

An ERTTX convenes DoD leaders and decision-makers, together with critical installation stakeholders, to work through a scenario that exploits the specific vulnerabilities and challenges facing that particular installation and the surrounding community. The scenarios are realistic and immersive, and are designed to provide specific new inputs throughout an exercise, according to a set formula:

- First, an apparent natural or accidental event causes a severe power outage on the installation, requiring immediate action.
- Later, it becomes clear that a determined adversary has caused the outage and is disrupting recovery efforts.
- Finally, it is revealed that the power grid will take multiple weeks to recover, requiring the installation and critical mission operators to plan for and activate long-term contingency plans.



Civil Engineering Squadron personnel prepare to shut down electrical power during an ERTTX, 19 November 2020.

ERTTX Outcomes

An ERTTX provides an installation with the opportunity to prepare for energy and mission disruptions. This kind of preparation can have a wide range of beneficial outcomes for the installation and larger DoD enterprise, including the following:

Develop a shared understanding of mission requirements

During an ERTTX, mission operators and installation support personnel work together to develop a common understanding of mission requirements, current energy resilience capabilities, and any gaps between requirements and capabilities. Due to the way that military installations are typically organized, installation support personnel do not often have an opportunity to understand the mission requirements of the building or infrastructure that they maintain. During an ERTTX, knowledge sharing happens organically, and when each stakeholder possesses the same knowledge, the installation as a whole will be more prepared to deal with prolonged regional electric power disruptions.

Challenge assumptions about critical infrastructure

ERTTXs highlight infrastructure gaps and potential impacts on military missions in the event of an evolving energy disruption. The exercise scenarios are created using information about an installation's infrastructure in conjunction with interviews with mission operators

and installation engineering staff to realistically test assumptions about how the infrastructure will hold up in a disruption.

Understand the consequences of a long-term disruption

Some longer-term impacts do not become apparent through the voluntary testing of backup power because such tests are executed only for a short duration (typically less than one hour). In contrast, an ERTTX provides the opportunity to think through how a long-term disruption, measured in days or weeks, would inevitably interrupt mission plans.

Justify funding for facility improvements

ERTTXs identify mission disruptions caused by insufficient infrastructure capability. When an installation's personnel confirm that a critical load is not supported by backup power through an energy resilience exercise, they have not only identified but also validated an energy resilience gap. These disruptions provide the justification and validation that is often required to secure funding for energy resilience improvement projects to increase infrastructure capabilities that will meet mission needs.

Prepare for a BSX

After completing an ERTTX, an installation may want to complete a BSX to validate some of the findings from the tabletop exercise. In addition, this real-world exercise will



Personnel prepare to shut down electrical power to a military base during an ERRTX in November 2020.

physically test different assumptions and highlight additional vulnerabilities and opportunities for infrastructure improvement projects.

Black Start Exercise

The key difference between an ERRTX and a BSX is the mechanics of the simulation. Each kind of exercise—one conducted in a conference room, the other involving the actual facility—prompts different questions, reveals different vulnerabilities, and stresses different capabilities. The two distinct processes are highly complementary and, when used together, reveal a more complete picture of an installation's resilience posture. An ERRTX will prompt discussions around how the installation *might* react to the scenarios and their consequences, while a BSX requires the installation's leadership and support staff to make real-time decisions to continue operations when installation power has actually been disconnected.

A Black Start Exercise requires the installation's leadership and support staff to make real-time decisions when installation power has actually been disconnected.

By simulating a scenario in which an installation is without commercial power for 6 to 24 hours, a BSX pushes installation personnel past assumptions into a controlled but realistic situation that can highlight unforeseen vulnerabilities. Most installations use a combination of diesel generators and uninterruptible power systems to provide backup power to their critical loads. However, the process of transferring critical loads to backup power is often not tested during normal operations. Without such testing under realistic conditions, there is no certainty that the backup power systems will in fact be able to start, transfer, and carry mission-critical loads when not connected to commercial utility power for an extended period of time. Executing a scenario in a controlled exercise environment allows installation personnel to address vulnerabilities in a

productive and safe manner before they face a real threat in an uncontrolled environment where mitigation might not be feasible.

BSXs test the ability of an installation's power system to function as designed, verify that the mission can function during a power disruption, and identify mitigation projects that will increase the mission's readiness posture. A successful BSX depends on strong installation and operational leadership support. A "no-notice" BSX provides the most value by testing the immediate response and performance of an installation's systems, people, and infrastructure under duress. BSXs use a four-phased approach to achieve these objectives:

Information collection: The exercise designers use data calls, interviews, and site visits to provide them with a functional understanding of an installation's infrastructure capabilities and mission requirements. This information is used by the designers to identify any gaps between the two.

Exercise development: Based on the information identified in the information collection phase, the exercise is constructed to highlight those gaps between requirements and capabilities. Exercises are scoped to include safeguards to prevent and protect against catastrophic failures to the installation.

Exercise execution: Installation personnel respond to the loss of commercial utility power and work to continue mission operations for multiple hours. Exercise observers document the identified gaps and potential areas that could be improved through project upgrades and process changes.

Outcome analysis and validation: Exercise observers and designers craft recommendations to improve installation resilience based on the exercise findings. Installation and operational leadership review the recommendations, event outcomes, and themes to prioritize the next steps.

The Outcomes of a BSX

The most basic benefit of intentionally disconnecting the commercial utility power for the installation is to test the ability of the backup systems to start, transfer, and carry the required loads. This is important because many installations do not consistently identify the electrical loads powering critical missions. In many instances, only specific organizations or individuals know where critical pieces of equipment such as network switches or alarm systems are located. Even when installations have identified their

critical loads, it is difficult to create a prioritized facility list that all tenant organizations know about and agree with. Broader benefits of BSXs include the following:

Developing a common understanding among stakeholders

Mission operators often work in organizational structures that are entirely separate from the infrastructure owners responsible for providing power to the missions. The exercise forces conversations and helps break down communication silos that previously may have kept mission operators from conveying their requirements to owners. The exercise also enables infrastructure owners to gain buy-in from mission operators to test the capabilities of the infrastructure systems. Thus, a well-planned BSX can increase communication among vital actors and lower barriers to cooperation.

A well-planned BSX can increase communication among vital actors and lower barriers to cooperation.

Understanding the immediate impact of a power outage

BSXs are executed over a range of 6 to 24 hours, often without notice, to test the immediate response of personnel and their ability to maintain the required level of mission readiness. Validating the speed and quality of a disaster response is particularly vital for missions that support warfighting capabilities.

Identifying gaps

BSXs expose areas where an installation's infrastructure capabilities fail to meet its mission requirements. This frequently happens when systems do not have the proper backup power equipment or there is a communication breakdown between stakeholders during the exercise. Typically, once leaders have had a window into the real-world consequences of infrastructure and process gaps and the potential implications for the mission if those gaps are not addressed, they are motivated to develop solutions that will strengthen mission continuity.

Justifying project funding

BSXs document the gaps in infrastructure requirements and demonstrate where energy resilience upgrades are most needed and where limited resources can be most effectively applied. The findings help decision-makers

determine which projects need immediate funding to support mission-critical operations and which can wait to be funded at some future date.

Resilience Exercise Results and Recommendations

Energy resilience exercises ensure policy compliance, identify mission requirements, map existing infrastructure and potential vulnerabilities, and generate engagement and discussions across organizations at an installation. Since 2015, DoD has completed more than 30 energy resilience site assessments and executed a variety of exercises.⁹ It is clear that there are consistent challenges and opportunities for installations regardless of the installation size, location,

their critical infrastructure and to better understand how they can serve an important customer in addition to the surrounding community.

These exercises are changing assumptions within the US military, most tangibly at the installations where they have been executed. Until recently, DoD took access to a reliable electrical system for granted; these exercises spotlighted the flaws in assuming that electrical power will always be available when needed. After participating in ERTTXs and BSXs, installation leaders have shared reactions such as, “You don’t even know what you need to be worried about until you start poking and prodding,” and “I am buying risk every day and I don’t know it.”¹⁰

Any company, organization, university, community, or nation that relies on power to maintain operations would benefit from executing an energy resilience exercise.

or military service. We know that our infrastructure is increasingly vulnerable because of extreme weather, outdated infrastructure, and heightened cyber attacks. These exercises allow each installation to understand its specific threats within those categories and work to strengthen its energy resilience posture.

Conclusion and Recommendations

Energy resilience exercises such as BSXs and ERTTXs are relatively new to DoD, but have already provided valuable information for both the participating installations and the US military community at large. But any company, organization, university, community, or nation that relies on power to maintain operations would benefit from executing an energy resilience exercise. The basic principles of such exercises remain constant no matter the kind or size of the organization that undertakes one, and they can raise stakeholder awareness of unsupported assumptions, faulty planning, and potential failures in energy systems in a controlled environment. The alternative is that these critical gaps in capabilities might otherwise go unnoticed until an actual disaster strikes.

These exercises also provide an opportunity for the organizations and stakeholders to understand their reliance on one another and the larger infrastructure systems. Mission operators, installation leadership, civil engineering departments, and exercise leaders at a military installation can push for energy resilience exercises to be included as part of their exercise curriculum and requirements. Installation utility providers can recommend a joint exercise to test

DoD must accelerate the process of shifting mindsets from making assumptions to conducting real-world exercises. This should include critical missions that were previously excluded from testing out of concern that even a controlled power loss would cause mission failure. The more important the mission, the greater everyone’s desire should be to test the system and validate that the mission will not fail during an actual outage. It is also likely that such an outage will not be isolated to the installation, but will also impact the surrounding community. Military installations are often seen as the beacon on the hill during a crisis, and the local community often houses much of the installation workforce. This is why community leaders are well positioned to advocate for a joint exercise that will identify ways in which the installation can support “beyond the fenceline” energy needs while ensuring mission continuity.

As “once in a lifetime” disasters occur more frequently and cyber attacks disrupt national critical infrastructure, understanding the military’s reliance on electric infrastructure becomes paramount.¹¹ Through energy resilience exercises, military leaders have an opportunity to understand how dependence on the electric grid affects mission readiness, and plan projects that will enhance mission assurance. These leaders must do what they can to advance the energy resilience training and exercises that will ensure mission readiness and enhance national security.

ABOUT THE AUTHORS

Adair Douglas is a Senior Associate at Converge Strategies.

Alex Pina is a Director at Converge Strategies.

Meredith Pringle is a Director at Converge Strategies.

This is a work of the US federal government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

9. Ariel Castillo, “Defense Energy Resilience Program” (PowerPoint presented at the Energy Exchange Conference, Denver, CO, August 2019): <https://oldcc.gov/sites/default/files/news/Agency-Resilience-Framework-Overview.pdf>
10. Nicholas Judson, “Resilience of Critical Missions for the Department of Defense” (PowerPoint prepared for US Air Force, 11 February 2020): [https://www.acq.osd.mil/eie/Downloads/IE/ERRE%20Presentation%2020200211INFORMS%20Final%20\(Distribution%20A\).pdf](https://www.acq.osd.mil/eie/Downloads/IE/ERRE%20Presentation%2020200211INFORMS%20Final%20(Distribution%20A).pdf)
11. Dan Charles, “Our Future On A Hotter Planet Means More Climate Disasters Happening Simultaneously,” NPR, 2 September 2021: <https://www.npr.org/2021/09/02/1033054816/our-future-on-a-hotter-planet-means-more-climate-disasters-happening-simultaneous>

NOTES

1. Garrett Hering, “US Power Outages Jumped 73% in 2020 amid Extreme Weather Events,” S&P Global, 19 January 2021: <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-power-outages-jumped-73-in-2020-amid-extreme-weather-events-62181994>
2. Created by Converge Strategies, LLC, 2021.
3. US Code Title 10, Subtitle A, Part 1, Chapter 1, § 101 (e)(6): “Energy Resilience,” Legal Information Institute, Cornell Law School: https://www.law.cornell.edu/uscode/text/10/101#e_6
4. *Climate Resilience: DOD Coordinates with Communities, but Needs to Assess the Performance of Related Grant Programs*, GAO-21-46 (Washington, DC: Government Accountability Office, 2020): <https://www.gao.gov/assets/gao-21-46.pdf>
5. Wilson Rickerson, Erin Brousseau, Meredith Pringle, Jonathon Monken, Jack Graul, Tom Calvert-Rosenberger, and Jack Barker, *Regulatory Considerations for Utility Investments in Defense Energy Resilience* (Washington, DC, and Boston, MA: Converge Strategies, LLC, 2021), <https://pubs.naruc.org/pub/9931AF59-1866-DAAC-99FB-17BF932AECF5>
6. Department of the Navy, *Department of the Navy Installation Energy Resilience Strategy*, (Washington, DC: Department of the Navy, 2020): <https://www.secnv.navy.mil/eie/Documents/DON-Installation-Energy-Resilience-Strategy.pdf>; Barbara M. Barrett, *Energy and Water Management*, Air Force Policy Directive 90-17 (Washington, DC: Department of the Air Force, 2020): https://static.e-publishing.af.mil/production/1/saf_ie/publication/afpd90-17/afpd90-17.pdf; Ryan D. McCarthy, “Subject: Army Directive 2020-03 (Installation Energy and Water Resilience Policy)” (official memorandum, Washington, DC: Department of the Army, 2020): https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN21689_AD2020_03_FINAL_Revised.pdf
7. Alex Beehler and J.E. Jack Surash, “Cutting the Cord to Test Energy Resilience,” US Army, 13 April 2020: https://www.army.mil/article/234514/cutting_the_cord_to_test_energy_resilience
8. National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong., 2nd sess. (15 December 2020): <https://www.govtrack.us/congress/bills/116/hr6395/text>



Energy in Conflict: The Case of the 2020 Armenia- Azerbaijan War

*Dr. Brenda Shaffer,
US Naval Postgraduate School*

WITH THE RISE IN FREQUENCY OF HYBRID warfare, combatants in various conflicts are increasingly targeting domestic energy infrastructure and energy supply flows.¹ In conventional warfare, militaries traditionally have sought to meet their operational energy needs, gain access to energy supplies, and deny energy supplies to their adversaries.² However, new energy-related elements of warfare have emerged. During the 2020 Armenia-Azerbaijan War, energy played several key roles. First, threats to energy infrastructure served as the trigger that ignited this round of hostilities: the war broke out on the eve of the commencement of operations of the Southern Gas Corridor, which would bring Europe its first new natural gas supply in decades. Second, energy infrastructure was also “weaponized” during the fighting, as has happened in warfare throughout history. Finally, Armenia targeted Azerbaijan’s energy export infrastructure during the war. This article will first analyze the energy factor in the 2020 Armenia-Azerbaijan War, and will then discuss the implications for future warfare.

Background: The Armenia- Azerbaijan Conflict

The wars between Armenia and Azerbaijan over control of the Nagorno-Karabakh region, especially the first war, from 1992 to 1994, have been among the most lethal conflicts between former Soviet states. During the Soviet period, Moscow had categorized Nagorno-Karabakh as an autonomous region in Soviet Azerbaijan, carving out its borders so that it created a region with an ethnic Armenian majority within Azerbaijan. This was a policy Moscow used to create division in many places in the USSR. When the Soviet Union collapsed in late 1991, all the new states recognized their existing Soviet-era borders as their new international borders, with the exception of Russia and Armenia. In this initial post-Soviet period, Russia occupied two regions of Georgia (Abkhazia and South Ossetia) and a region of Moldova (Transnistria).³ Armenia invaded Azerbaijan and captured the Nagorno-Karabakh region and seven additional regions of Azerbaijan, all of which had been recognized by the international community (including the United States) as part of Azerbaijan’s legal territory. Yerevan expelled all the non-Armenian population from the occupied territories, creating close to 800,000 new Azerbaijani refugees. The conflict left the region economically shattered for years.

Russia stoked the conflicts, especially the first war, because the state of belligerence rendered the two combatants more vulnerable to coercion by Moscow.⁴ While Moscow did not formally recognize Yerevan's control of Nagorno-Karabakh and the surrounding seven districts, it used the conflict to reinforce its power in the region by maintaining two military bases in Armenia and controlling Armenian airspace and air defenses. Moreover, Armenia is a member of the Collective Security Treaty Organization, the Russian-led mutual defense pact.

Yerevan referred to the areas it occupied as the “Nagorno-Karabakh Republic,” even though Armenian military forces occupied the regions.

Armenia copied Moscow's playbook in the regions it occupied, trying to convince the international system that these regions were under the sovereignty of independent entities instead of under occupation.⁵ Thus, Yerevan referred to the areas it occupied as the “Nagorno-Karabakh Republic,” even though Armenian military forces occupied the regions, Yerevan provided the budget for the regions, all the local officials were citizens of Armenia, and many had served as senior Armenian officials.⁶ During the Armenian occupation, Yerevan established settlements in Nagorno-Karabakh and provided financial and other incentives to ethnic Armenians, especially those from Lebanon and Syria, to move to the occupied territories. Officials in Armenia, local authorities in Nagorno-Karabakh, and diaspora organizations flaunted their efforts to bring settlers to the occupied territories.⁷

In the period following the first war, the line of contact between the forces of Armenia and Azerbaijan remained tense, with an average of over a dozen soldiers killed each year. From time to time, the conflict flared up into full battles, including one in April 2016 that became known as the “Four-Day War” and led to over 200 deaths.

Energy Exports

Azerbaijan is a major source of energy resources, most of which are exported to Europe. Over the last fifteen years, it has produced between 750,000 and one million barrels of oil a day. In 2006, Azerbaijan also began to export natural gas to Georgia and Turkey. In late 2020, following the second Armenia-Azerbaijan War, Azerbaijan opened the Southern Gas Corridor (SGC), which brings natural gas from the Caspian Sea region to Europe; this project was the first new source of pipeline natural gas for

Europe in several decades. While the SGC supplies less than 10 percent of Europe's gas imports, it has enabled specific states—Italy, Greece, and soon, Bulgaria—to diversify their gas supplies and thus greatly reduce their dependence on Russia.⁸ The SGC is anticipated to carry additional gas volumes from fields in Azerbaijan and also potentially from other producers in Central Asia and the Eastern Mediterranean in the future. It is intended to turn Azerbaijan into a major supplier of energy to Europe and provide Baku with a new revenue stream that would improve Azerbaijan's strategic position.

Energy: The Catalyst for Reigniting War

In 2020, full-scale war reignited between Armenia and Azerbaijan, when Armenia launched a surprise attack several weeks before Azerbaijan was due to begin commercial operation of the SGC.⁹ The first phase of the 2020 Armenia-Azerbaijan War began on July 12 in the Azerbaijani region of Tovuz, along the northern section of the international border between Armenia and Azerbaijan. This region is located 300 kilometers north of what had been the line of contact between Armenia's and Azerbaijan's forces in the occupied territories. In the initial attacks, Armenian troops attempted to gain control of Azerbaijan's Qaraqaya Heights, which are perched above the energy and transit corridor that runs from the Caspian Sea to Europe and includes the SGC. Since Armenian control of the Heights would have allowed Yerevan to threaten the energy and transit corridor, the attacks posed a strategic threat to Azerbaijan.

Armenian troops attempted to gain control of Azerbaijan's Qaraqaya Heights, above the energy and transit corridor that runs from the Caspian Sea to Europe.

A member of the Armenian Special Forces who was captured in Azerbaijan stated during his trial that his unit had been ordered to attack the Azerbaijani section of the Baku-Tbilisi-Ceyhan oil pipeline during the July 2020 fighting:

During the Tovuz battles, there was such a combat mission. The Central Command ordered us to explore the protected areas in that area. In connection with the order to blow up the oil pipeline, I marked the positions of the Azerbaijani Army on the map and calculated the protected areas. I made notes on maps and documents and handed them over to the relevant authorities.¹⁰

Amid such threats to the energy corridor's security, new investments in its expansion were unlikely. Thus, the July 2020 Armenian attacks risked devaluing the corridor and undermining Azerbaijan's ability to receive strategic benefits as a gas supplier to Europe.

Armenia chose the timing and location of the attacks deliberately to create the impression that it has the capacity to disrupt this strategic energy and transit corridor at will. As Elshad Nasirov, Vice President for Marketing and Investments of SOCOR, the State Oil Company of the Azerbaijan Republic, pointed out at the time, "it is not by chance that Armenia launched a military operation against Azerbaijan three months before the start of Azerbaijani gas supplies to Europe."¹²



Map of the Southern Gas Corridor, consisting of Southern Caucasus pipeline (SCP), Trans-Anatolian gas pipeline (TANAP), Trans-Adriatic pipeline (TAP).

Following the July 2020 attacks in Tovuz, senior Armenian officials stated that Armenia's goal was to make it clear to the EU that "Armenia is the guarantor" of Europe's energy security.¹¹ In August 2020, Armenian representatives stated that, in light of the fighting, Armenia planned to coordinate with the EU's Directorate General for Energy on the security of the supplies to Europe, and that Yerevan planned to claim that the security of the corridor was now in Armenia's hands. In this way, Armenia sought not only to increase its importance in Brussels by emphasizing its ability to disrupt gas supplies to Europe, but also to threaten Azerbaijan's extensive investment in the SGC.

Hikmet Hajiyev, foreign policy advisor to Azerbaijan's President Ilham Aliyev, also referred to the link between the location of the attacks and the planned commencement of the major gas exports to Europe:

It was not coincidental why Tovuz was chosen as a venue to carry out a military provocation against Azerbaijan in July 12–16, 2020. Tovuz is situated on [sic] international border between Armenia and Azerbaijan, not along the Line of Contact, and hosts energy and infrastructure projects nearby. The Baku–Tbilisi–Supsa and BTC oil pipelines, and the

Southern Caucasus pipeline, an important chain in the multimillion dollar megaproject the Southern Gas Corridor (SGC), pass close by the Tovuz area. The intention of Armenia to engage third parties in the war against Azerbaijan and demolish the latter's critical energy infrastructure was also present in July.¹³

In parallel with the attacks at Tovuz, Armenian troops shelled Nakhchivan, an Azerbaijani exclave. This attempt to open new fronts was in line with Armenia's then-Defense Minister Davit Tonoyan's doctrine of "New Wars for New Territories."¹⁴ According to Tonoyan's doctrine, Armenia sought to expand the arenas of fighting between Armenia and Azerbaijan in order to deter Azerbaijan from retaking control of occupied Nagorno-Karabakh and surrounding territories.

Armenia's attempt to gain control of the hills above the Southern Gas Corridor is in line with its strategy, which views Azerbaijan's energy production and export infrastructure as key military targets. Over three decades of conflict, Armenian leaders had openly threatened to attack Azerbaijan's oil and gas production and export pipelines, and Armenian military exercises frequently simulated such attacks.¹⁵

The energy aspects of the Armenia-Azerbaijan conflict are exceptional because belligerents traditionally target energy supplies in order to deny an adversary access to energy. In this conflict, however, Armenia targeted Azerbaijan's energy export infrastructure in order to deny it the strategic benefits of serving as an export state to Europe. In addition, as an ally of Russia, Armenia may also have been operating to prevent new energy resources from arriving in Europe that could challenge Moscow's energy dominance.

Armenia targeted Azerbaijan's energy export infrastructure in order to deny it the strategic benefits of serving as an export state to Europe.

The new strategic reality that emerged in July 2020, with the opening of two additional fronts with Armenia and a threat overhanging the strategically important energy and transport corridor to the West, was unsustainable. Through the attacks in Tovuz, Yerevan had created a *casus belli*. By opening a new front and attempting to neutralize Azerbaijan's emerging role as an energy provider to Europe, and thus deny new revenues to Baku, Armenia set the stage for the eruption of full-scale war in late September 2020.

Attacks on International Pipelines during the War

In retrospect, the July 2020 Tovuz attacks were the first phase of the Second Armenia-Azerbaijan War. In the second phase of the war, beginning 27 September 2020, Armenia continued to threaten Azerbaijan's energy pipelines. In October 2020, Armenia fired missiles that landed within 10 meters of the Baku-Tbilisi-Ceyhan (BTC) oil pipeline, near the Azerbaijani city of Yevlax.¹⁶ However, these missile attacks did not disrupt the operations of the BTC or other nearby pipelines.

The 2020 Armenia-Azerbaijan War was not the first time that Armenia threatened or attempted to attack Azerbaijan's energy production and export infrastructure. Similar threats were made, for instance, during clashes between the two countries in April 2016.¹⁷ Serzh Sargsyan, who was the president of Armenia at the time, later criticized Prime Minister Nikol Pashinyan for not using the sophisticated Russian-built Iskander ballistic missiles in Armenia's arsenal to attack the pipelines, saying, "in the end, why did we buy these missiles? Not to use at the right time? The Iskanders are ours, and we are the only ones to whom [Russia] gave such weapons. And we didn't use them."¹⁸ While the Iskander missiles were not used to attack the pipeline corridor, Armenia did fire them at Azerbaijani troops in Shusha toward the end of the autumn 2020 war.¹⁹

Weaponization of Energy Infrastructure

The Second Armenia-Azerbaijan War featured several elements of hybrid warfare, including the intentional targeting of civilian populations (such as the Armenian missile attacks on the Azerbaijani cities of Barda and Ganja), and extensive media and disinformation campaigns. As part of this hybrid warfare, Armenia and Azerbaijan both threatened to "weaponize" energy infrastructure in each other's state and unleash mass civilian casualties. The goal in weaponizing energy infrastructure is not just to disrupt energy supplies, but also to create significant damage and potential loss of life through attacks on pipelines, power plants, grids, and other energy infrastructure elements. As part of this policy, Armenia threatened to attack the Mingachevir hydropower station, which would have led to massive flooding, in addition to crippling Azerbaijan's electricity supplies. Baku, in turn, threatened to respond to such an attack by attacking Armenia's Metsamor nuclear power plant, although a senior Azerbaijani official later walked back this threat.



A view of a destroyed house after attacks carried out by the Armenian army with heavy weapons in Dondar Kuscu village of Tovuz.

Armenia's Threats to the Mingachevir Hydropower Station

Historically, many armies have used intentional flooding as a military tactic.²⁰ Chinese forces intentionally flooded the Yellow River in their war with Japan in 1938, leading to hundreds of thousands of deaths and the displacement of millions more.²¹ In the Iran-Iraq War of the 1980s, Iraq used intentional flooding to deny access to the battle zones.²² Most recently, Ukrainians apparently flooded fields north of the capital, Kyiv, to slow the advance of Russian invading forces in March 2022.²³ Concerns continue that ISIS and other terrorist groups could attack the Mosul Dam to flood areas in Iraq. For decades, Armenia has threatened to attack the Mingachevir hydropower station in Azerbaijan. A successful attack on the facility that caused the release of high volumes of water would result in significant casualties and turn large areas of Azerbaijan into uninhabitable and uncultivable land. It would also hinder operation of the east-west energy and transportation corridor that runs close to the Mingachevir region.

Following clashes between Armenia and Azerbaijan in 2014, Armenian Defense Minister Seyran Oganyan threatened an attack on the Mingachevir Dam. These threats were renewed in July 2020, when a representative of Armenia's Ministry of Defense threatened to use SU-30 fighter jets and Iskander ballistic missiles to attack the dam.²⁴ During the second stage of the 2020 war, Armenia made good on its threat and fired four Tochka U short-range missiles at the city of Mingachevir, which sits at the base of the Mingachevir Dam.²⁵ The missiles were intercepted by Azerbaijan's air defenses before they reached their target, but the incident made clear that Armenia was willing to attack the dam and potentially cause massive flooding in Azerbaijan. Accordingly, during the war, the Azerbaijani government lowered the water level in the Mingachevir reservoir and at several other hydropower plants in Azerbaijan.

Azerbaijan's Threat to the Metsamor Nuclear Power Plant

In July 2020, Azerbaijani Colonel Vagif Dargahli, a spokesman for the Defense Ministry, said this in response to the Armenian threat to attack the Mingachevir Dam:

This attack [on the Mingachevir Dam] is impossible due to the relief of the territory where which [sic] this strategic facility is located, the fortifications, as well as the Azerbaijani Air Forces' modern air defense systems. . . . Armenia must not forget that the latest missile systems in the arsenal of the Azerbaijani army can target and launch an attack on its Metsamor nuclear power plant, which may lead to a major disaster for Armenia.²⁶

Armenia's nuclear power plant is located only 35 kilometers from Yerevan, and 16 kilometers from the Turkish city of Iğdır. An attack on Metsamor would endanger not only the people of Armenia, but also those who live in the wider region, including Turkey, Georgia, and Azerbaijan itself.²⁷ Thus, this was not a credible threat. Presidential advisor Hikmet Hajiyev later walked it back, stating that the Defense Ministry spokesman had made an unauthorized statement, and that Azerbaijan had no intention of attacking the Metsamor nuclear power plant or any other civilian infrastructure in Armenia: "During the latest provocations different misinformation was spread. . . . Azerbaijan does not have the policy to target any critical strategical facilities."²⁸ However, it is clear that during the 2020 Armenia-Azerbaijan War, energy infrastructure was viewed not only as a potential target but also effectively as a potential weapon that could be leveraged to deter the adversary. Azerbaijan drew lessons and Baku has undertaken steps to strengthen defense of the country's energy infrastructure, including the Mingachevir Dam.

Energy infrastructure was viewed not only as a potential target but also effectively as a potential weapon that could be leveraged to deter the adversary.

Energy Trade Post-War

Azerbaijan's decisive victory in the war strengthened the security of the international export pipelines and created opportunities for new energy flows in the region. Armenia's defeat removed the threat to Azerbaijan's oil and natural gas pipelines, and full operation of the SGC commenced on schedule in December 2020. In addition, most of the major players are striving for a post-war regional

architecture that will enable new regional cooperation, including common roads and rail transit, the opening of borders, and, potentially, new energy flows.²⁹

New post-war road and rail transport links connecting Armenia to Azerbaijan and Turkey would improve Armenia's energy security by allowing it to import more diverse energy supplies, such as coal and oil, via Turkey. Coal and oil are easy to stockpile and could be used to back up Armenia's gas network. Having access to new energy sources could allow Armenia to close the Metsamor nuclear power plant. A Soviet-era nuclear power plant, Metsamor is one of only five reactors still in operation that lack a containment vessel; moreover, it is located in a major seismic zone. Any accident at Metsamor would pose a serious threat to Armenia, its neighbors, and southern Europe.³⁰ Thus, shutting down the plant would be in the best interests of all parties concerned.

Conclusions

The 2020 Armenia-Azerbaijan War was the first full-scale interstate war in the twenty-first century. Western (Turkish/NATO and Israeli) weapons systems squared off against Russian systems, and the Western systems unquestionably prevailed. Many strategists and military planners are studying this war, which featured new uses of weapons such as UAVs. The conflict also witnessed the extensive use of hybrid warfare, including Armenia's intentional targeting of civilian populations outside the war zone, and active media campaigns on both sides.

As discussed in this article, the hybrid warfare also included several elements connected to energy, some of which were novel. These include Armenia's attempts to threaten Azerbaijan's oil and natural gas export pipelines. Both sides also threatened to turn parts of their opponent's power generation systems against them. While targeting power generation and causing intentional flooding are not new to warfare, threats and attacks on major energy infrastructure pieces—such as dams and nuclear power plants—indicate that the weaponization of energy infrastructure is likely to play a major role in contemporary hybrid warfare and should be studied further.

The weaponization of energy infrastructure is likely to play a major role in contemporary hybrid warfare and should be studied further.

Moreover, the threats and attacks on the Mingachevir Dam are a reminder to military planners and strategists that intentional flooding is still a threat. Thus, they need to develop both doctrine and mechanisms, such as air defenses, to neutralise these sorts of threats against critical energy infrastructure. In the future, Azerbaijan seems likely to acquire advanced air defense systems like Iron Dome to protect elements of its energy infrastructure, a practice that is likely to become more prevalent in combat zones around the globe.

In future warfare, attacks on domestic energy infrastructure will not only take place physically, as witnessed in the Second Armenia-Azerbaijan War, they will also likely take the form of cyber attacks, since all modern energy infrastructure is managed by cyber systems. The hybrid aspects of the Second Armenia-Azerbaijan War, and especially the attacks on Azerbaijan's domestic energy infrastructure, are reminders that the borders between the battlefield and the domestic arena, including both citizens and energy infrastructure, have become blurred. War planners will need to continue to plan for protection of the domestic arena during time of war.

ABOUT THE AUTHOR

Dr. Brenda Shaffer is a research faculty member of the Energy Academic Group at the US Naval Postgraduate School.

This is a work of the US federal government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

NOTES

1. This article is based on a previously published book chapter by the author: Brenda Shaffer, "The Trigger for War: Energy in the 2020 Armenia-Azerbaijan War," in *The Karabakh Gambit: Responsibility for the Future*, ed. Turan Gafarli and Michael Arnold (Istanbul: TRT World Research Centre, 2021), 100-114.
2. Operational energy is the "energy required for training, moving, and sustaining military forces and weapons platforms for military operations." 2010 Quadrennial Defense Review, section 138c, as cited in Department of Defense, *Energy for the Warfighter: Operational Energy Strategy* (Washington, DC: Department of Defense, 2011), 3: <https://apps.dtic.mil/sti/pdfs/ADA544100.pdf>
3. In 2014, Russia also captured Crimea from Ukraine, formally annexed it, and occupied Ukraine's Donbas region.
4. On the Armenia-Azerbaijan conflict, see Svante E. Cornell, *Small Nations and Great Powers: A Study of Ethnopolitical Conflict in the Caucasus* (London: RoutledgeCurzon, 2001); Thomas de Waal, *Black Garden: Armenia and Azerbaijan Through War and Peace* (New York: New York University Press, 2013); and Svante E. Cornell, ed., *The International Politics of the Armenian-Azerbaijani Conflict: The Original "Frozen Conflict" and European Security* (New York: Palgrave, 2017).
5. For more on Russia's and Armenia's use of proxies to attempt to evade responsibility for occupying other countries, see Svante E. Cornell and Brenda Shaffer, "The United States Needs to Declare War on Proxies," *Foreign Policy*, 27 February 2020: <https://foreignpolicy.com/2020/02/27/russia-iran-suleimani-the-united-states-needs-to-declare-war-on-proxies/>
6. See Svante Cornell and Brenda Shaffer, *Occupied Elsewhere: Selective Policies on Occupations, Protracted Conflicts, and Territorial Disputes* (Washington, DC: Foundation for Defense of Democracies, 2020), 22-23.
7. Edik Baghdasaryan, "Repopulation is An Essential Question for All Armenians," *Hetq*, 25 June 2007: <https://hetq.am/en/article/6744> ; Melania Harutyunyan, "Deputy Prime Minister of Artsakh Spoke about the Resettlement of Artsakh," *Aravot*, 27 July 2013: <https://www.aravot-en.am/2013/07/27/155729>
8. For more on the significance of Caspian energy, see Brenda Shaffer, "In the Era of U.S. Energy Abundance: The Role of the Caspian Region in U.S. Policy," *The Brown Journal of World Affairs* 26, no. 2 (spring/summer 2020): <https://bjwa.brown.edu/26-2/in-the-era-of-u-s-energy-abundance-the-role-of-the-caspian-region-in-u-s-policy/> ; Brenda Shaffer, "Gas Politics After Ukraine: Azerbaijan, Shah Deniz, and Europe's Newest Energy Partner," *Foreign Affairs*, 17 December 2013: <https://www.foreignaffairs.com/articles/russia-fsu/2013-12-17/gas-politics-after-ukraine>
9. Brenda Shaffer, "Armenia-Azerbaijan Conflict Poses Threat to European Energy Security," *FDD*, 17 July 2020: <https://www.fdd.org/analysis/2020/07/17/armenia-azerbaijan-conflict-energy-security/>
10. "Armenian Citizen Accused of Terrorism: 'We were Instructed to Explode Baku-Tbilisi-Jeyhan Pipeline,'" *APA*, 10 January 2022: <https://apa.az/en/incident/armenian-citizen-accused-of-terrorism-we-were-instructed-to-explode-baku-tbilisi-jeyhan-pipeline-365617>
11. "Армения опровергла планы по атаке нефтегазовой инфраструктуры Азербайджана" [Armenia Denies Plans to Attack Azerbaijan's Oil and Gas Infrastructure], *lenta.ru*, 19 July 2020: <https://lenta.ru/news/2020/07/19/armenia/>

12. "Elshad Nasirov: Armenian Provocation is a Threat to Azerbaijan's Energy Infrastructure," *Azerbaijan24*, 17 July 2020: <https://www.azerbaijan24.com/en/elshad-nasirov-armenian-provocation-is-a-threat-to-azerbaijan-s-energy-infrastructure/>
13. Hikmat Hajiyev, "Attacks by Armenia Against Azerbaijani Civilians and Critical Infrastructure Should not be Overlooked," *Euractiv*, 30 October 2020: <https://www.euractiv.com/section/azerbaijan/opinion/attacks-by-armenia-against-azerbaijani-civilians-and-critical-infrastructure-should-not-be-overlooked/>
14. "We Do the Opposite – New War for New Territories: Minister Tonoyan's Tough Statement," *Lragir.am*, 30 March 2019: <https://www.lragir.am/en/2019/03/30/71511> ; "Pashinyan Backs Defense Chief's Tough Talk on Karabakh," *The Armenian Mirror-Spectator*, 2 April 2019: <https://mirrorspectator.com/2019/04/02/pashinyan-backs-defense-chiefs-tough-talk-on-karabakh/>
15. Sargis Harutyunyan, "Missile Strikes on Oil Facilities Simulated in Armenian War Games," *Azatutyun*, 15 October 2012: <https://www.azatutyun.am/a/24740508.html>
16. David O'Byrne, "Major Caucasus Oil, Gas Pipelines Unaffected by Rocket Attack: Azerbaijan's Socar," *S&P Global/Platts*, 7 October 2020: <https://www.spglobal.com/platts/en/market-insights/latest-news/natural-gas/100720-major-caucasus-oil-gas-pipelines-unaffected-by-rocket-attack-azerbaijans-socar> ; "BP Works on Reinforcing Security at Azerbaijan Facilities," *Reuters*, 7 October 2020: <https://www.reuters.com/article/armenia-azerbaijan-bp-int/bp-works-on-reinforcing-security-at-azerbaijan-facilities-idUSKBN26S27U>
17. "СРОЧНО! Карабах готов нанести удар по нефтяным коммуникациям Азербайджана" [URGENT! Karabakh Ready to Strike at Azerbaijan's Oil Communications], *NewsArmenia*, 5 April 2016: https://newsarmenia.am/news/nagorno_karabakh/srochno-karabakh-gotov-nanesti-udar-po-neftyany-kommunikatsiyam-azerbaydzhana/
18. "Ex. Armenian Pres. Sargsyan Hurls New Accusations at Pashinyan Gov't," *JAMnews*, 17 February 2021: <https://jam-news.net/ex-armenian-pres-sargsyan-hurls-new-accusations-at-pashinyan-govt/>
19. Mushvig Mehdiyev, "Fragments of Iskander Missile Found in Azerbaijan's Karabakh Region Raise Serious Questions," *Caspian News*, 4 April 2021: <https://caspiannews.com/news-detail/fragments-of-iskander-missile-found-in-azerbaijans-karabakh-region-raise-serious-questions-2021-4-4-0/>
20. Stanley W. Dziuban, "Implications of Artificial Flooding in Military Operations," *The Military Engineer* 42, no. 285 (January-February 1950), 13-15: https://www.jstor.org/stable/44561030?seq=3#metadata_info_tab_contents
21. F. Tillman Durdin, "Chinese Attacking Japanese in Flood," *New York Times*, 13 June 1938: <https://timesmachine.nytimes.com/timesmachine/1938/06/13/98149691.html?pageNumber=1>
22. "Iran Seeking to use Water as a Weapon," *Chicago Tribune*, 12 March 1987; Michael Sterner, "The Iran-Iraq War," *Foreign Affairs* (Fall 1984): <https://www.foreignaffairs.com/articles/iran/1984-09-01/persian-gulf-iran-iraq-war> ; Javed Ali, "Chemical Weapons and the Iran-Iraq War: A Case Study in Noncompliance," *The Nonproliferation Review* (Spring 2001): 43–58: <https://www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf>
23. Reis Thebault and Dylan Moriarty, "Satellite Images Show Flooding North of Kyiv in Possible Sign of 'Hydraulic Warfare,'" *Washington Post*, 9 March 2022: <https://www.washingtonpost.com/world/2022/03/09/ukraine-intentional-flooding/>
24. Hajiyev, "Attacks by Armenia against Azerbaijani Civilians and Critical Infrastructure."
25. Ibid.
26. "Azerbaijan Responds to News on Armenia Targeting to hit Mingachevir Reservoir," *Trend News Agency*, 16 July 2020: <https://en.trend.az/azerbaijan/politics/3270655.html>
27. Brenda Shaffer, "Armenia's Nuclear Power Plant is Dangerous. Time to Close It," *Bulletin of the Atomic Scientists*, 5 March 2021: <https://thebulletin.org/2021/03/armenias-nuclear-power-plant-is-dangerous-time-to-close-it/>
28. "Hikmat Hajiyev: 'Armenia has Deliberately Turned Metsamor Issue Which Poses Serious Threat for Region, into Show,'" *APA*, 21 July 2020: https://apa.az/en/nagorno_garabagh/Hikmat-Hajiyev:-%22Armenia-has-deliberately-turned-Metsamor-issue-which-poses-serious-threat-for-region-into-show%22-326277
29. "Pashinyan Says Armenia is Ready to Restore Road Communication with Azerbaijan," *International News.az*, 9 February 2022: <https://news.az/news/pashinyan-says-armenia-is-ready-to-restore-road-communication-with-azerbaijan>
30. Shaffer, "Armenia's Nuclear Power Plant is Dangerous."



The Integration of Special Forces in Cyber Operations

*LTC Jonas van Hooren,
Netherlands Ministry of Defense*

THE VAST SOCIETAL AND TECHNOLOGICAL changes that characterize the Information Age, such as the so-called “Internet of Things,” a more interconnected world, and faster and better digital networks, have both enriched and imperiled humanity. The four traditional operational environments of land, maritime, air, and space are now inextricable from a new, fifth domain: the information environment, or cyberspace. The cyber domain encompasses all forms of electronic, server-based activity, including “digital warfare.”¹

Unlike the four natural domains, the cyber domain’s lack of boundaries, transparency, and sovereign jurisdictions can make it an environment of lawlessness, one which increasingly facilitates criminality and terrorism. No individual country has absolute sovereignty within the digital domain, but because everyone depends on access to cyberspace, most countries agree on best behaviors to protect these areas. However, there are a number of bad actors and opportunists who are willing to exploit the digital commons for their own gain at the expense of others.

Using the Netherlands as a case study, this article investigates ways by which militaries could institutionalize and encourage a potentially symbiotic relationship between their special forces capabilities and cyber assets at the strategic level, and the impact such a relationship could have at the operational and tactical levels of hybrid conflict.² The research focuses on military exploitation of offensive, defensive, and intelligence cyber assets, and explores the possible roles SOF can play to support cyber operations. If integration of the two activities is carried out incrementally and with full awareness of both obstacles and opportunities, both SOF and cyber can innovate, reinforce, and

learn together to be more effective. Although this article focuses on the Netherlands's institutions and capabilities, these findings can also be useful to a broader audience. For example, in 2021, Dutch SOCOM formed a Composite Special Operations Component Command (C-SOCC) with Belgium and Denmark as a NATO Response Force (NRF). This C-SOCC, which will probably change to a more regional focus within the next few years, offers opportunities to explore NATO's SOF and cyber capabilities in a multinational and multidomain environment.³

The New Age of Hybrid Threats

Cyberspace is already integral to warfighting (think GPS), and it will have a powerful effect on the future of the military, especially SOF, because both worlds are becoming more closely intertwined. The difference between soldiers using real guns and hackers pulling a zero-day trigger online is dissolving.⁴ Automated algorithms designed to wield autonomous weapons in combat without direct human intervention or oversight, for example, would be a perfect tool for a hacker to manipulate to turn an armed force against itself. It is equally easy to imagine perpetrators hacking one enemy and misleading it into attacking another enemy, all while claiming plausible deniability and never entering the physical conflict zone themselves.

There is no universally accepted definition of what constitutes a hybrid threat, so it is difficult to describe precisely the current hybrid threats to the Netherlands or any other nation.⁵ Nevertheless, certain elements are typically involved, such as the integration of both conventional and non-conventional military forces, and various non-military means to conduct destabilizing activities against targets. For example, unidentifiable groups, such as unmarked special forces, proxies, private military organizations, and volunteers might engage in quasi-military operations in combination with diplomatic, economic, and informational activities to undermine another state's stability and sovereignty. State and non-state actors have historically used a mixture of such means to influence, manipulate, disinform, and control; in this sense, there is nothing new about hybrid warfare. It is the recent addition of the cyber domain to the mix that makes hybrid threats both global in nature and uniquely current.

It is the recent addition of the cyber domain to the mix that makes hybrid threats both global in nature and uniquely current.

The cyber domain gives nation-states the opportunity to counter national threats under the radar, and SOF could be a proficient capability to support these cyber acts. Special operations forces are specially selected, trained, and equipped for ambiguous conflicts everywhere in the world.⁶ NATO doctrine assigns three primary roles to special forces: special reconnaissance (SR), military assistance (MA), and direct action (DA).⁷ While these three main tasks, or derivatives of them, are traditionally executed in the physical landscape, the cyber domain gives SOF opportunities to counter hybrid threats and, on the physical level, validate proposed data and actions that are communicated virtually. The physical role SOF currently plays in hybrid warfare will necessarily evolve when future forms of warfare take place primarily online. Thus, SOF could be the global human link between the physical environment and the virtual cyber domain.

Possible SOF Roles in Cyber Operations

SOF's characteristics make them an effective and dynamic tool for cyber operations, with the ability to support cyber operations by "small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign (cyber) policy."⁸ SOF personnel are trained to blend in with the local civilian environment while conducting overt, covert, or clandestine low-visibility operations in hostile and even denied areas. This is where SOF distinguish themselves from human intelligence operators. SOF can conduct operations of long duration and have the endurance and persistence to operate independently from support and supplies in any environmental circumstance in the world.

Dutch SOF can be used in three distinct roles to support cyber operations initiated by the Defense Cyber Command (DCC) and the Joint SIGINT Cyber Unit (JSCU): (1) gain access to hard targets for cyber operations; (2) provide the means to get people, hardware, and software into or out of the operational area; and (3) understand, deceive, and influence the cultural environment. As in many NATO countries, Dutch SOF characterize themselves as a joint strategic asset that can "conduct special operations in uncertain, hostile, or politically sensitive environments to create effects

that support the achievement of strategic-operational comprehensive objectives. These operations may be conducted using clandestine or covert capabilities/techniques and require mature and highly-trained operators.”⁹ Although SOF are certainly not an answer to every cyber problem and gap, and some roles will not be useful in every cyber-centric operational environment, these possibilities should at least be considered in the planning of cyber operations.

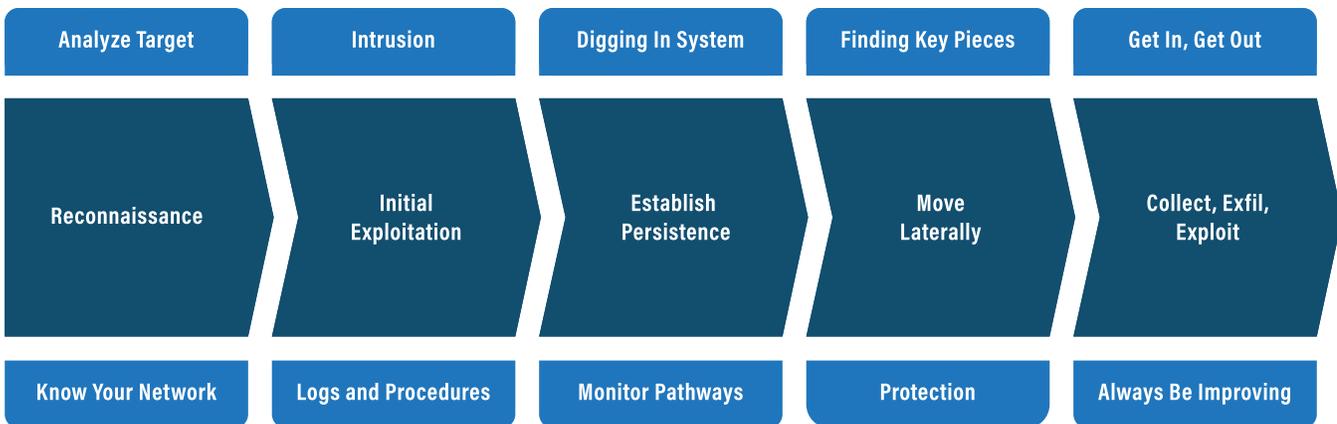
The three proposed roles for SOF in cyber operations—access, insertion/extraction, and environmental influence—differ significantly, but they are not mutually exclusive.

The three proposed roles for SOF in cyber operations—access, insertion/extraction, and environmental influence—differ significantly, but they are not mutually exclusive, and it is easy to imagine how they might overlap. For example, before a cyber technician can be extracted out of a hostile environment (role 2), SOF first need to understand, de-

entry was needed to gain access to these so-called “hard targets.”¹⁰ SOF’s character as a clandestine operating force, capable of blending in with the local community and equipped with the proper reconnaissance, sabotage, breach, and fighting tools, make it a valuable support for such cyber operations. Once SOF have breached a hard target, it becomes possible for tech experts, either specially trained SOF personnel themselves or embedded cyber specialists, to access and break into the computers, networks, and information systems in or around the target site or to simply physically exploit tactical sites.¹¹

Hacking into computers through active cyber operations is often executed via an intrusion model. The model is not technically or tactically focused, but could be used as an operational concept for intruders to reach their strategic objects in cyber operations.¹² Each stage (reconnaissance, initial exploitation, establishment of persistence, lateral moves, and collection-exfiltration-exploitation) in this model presents an opportunity to get deeper in someone’s system to spy, influence, sabotage, collect, or even attack. Figure 1 illustrates the intrusion model and the stages of this multifaceted process.¹³

ATTACKER’S FOCUS



DEFENDER’S METHOD

Figure 1: The Intrusion Model¹⁴

ceive, and perhaps influence the cultural environment (role 3) in preparation for the extraction. As it is, each role could serve as an umbrella for numerous kinds of SOF operations using various tactics, techniques, and procedures.

Access Hard Targets for Cyber Operations

The planning, execution, and command and control of cyber operations could, at least in theory, be handled from any connected platform—land, air, sea, or space—in the world. There have been times, however, where physical

Especially in the first stages of the intrusion model, SOF could conduct SR to collect information on the target (target acquisition) or be the initial entry force to bridge the “air gap” between the physical and virtual environments. In such proximity, SOF could collect intelligence about the target and use radio-frequency technology to establish a connection with objects of interest, including those that are isolated from the internet.¹⁵ At this point, the cyber experts “back home” on whatever platform was guiding the operation could exploit the gathered intelligence and prepare for the next stage in the intrusion

model. Human assets, like intelligence operators, can collect intelligence and deliver digital malware like viruses, spyware, worms, Trojan horses, or ransomware without being physically connected to the internet.

Another possible scenario involves SOF's ability to infiltrate and emplace physical devices in sensitive foreign locations to intercept, gather, corrupt, disrupt, or jam data flows. In 2012, for example, when an Iranian Islamic Revolutionary Guard unit was moving what seemed like an ordinary rock near the underground Fordow nuclear enrichment plant, the rock exploded, revealing spyware that had been hidden inside it.¹⁶ SOF are the human tool that can bridge air gaps with technical equipment, especially in denied and hostile circumstances.

Move Assets Into or Out of the Operation Area

In the land, air, and maritime domains, Dutch SOF are able to operate covertly using a wide variety of techniques, vehicles, and devices. These capabilities allow Dutch SOF to function as an SR element, quick reaction force, counterterrorism unit, or force protector to support cyber operations. SOF have the ability not only to infiltrate humans, including technical cyber experts or support agents, into and extract them from a hostile environment, but also to catch and arrest hackers, cyber criminals, or cyber terrorists in the act as they sit behind their computers or use their mobile devices. Once the culprits are in hand, SOF can extract such individuals, including their software and hardware, and turn everything over to the local authorities for forensic exploitation and possible legal action.

SOF have the ability to infiltrate humans, including technical cyber experts or support agents, into and extract them from a hostile environment.

As with humans, it is also possible for SOF to insert software and/or hardware into a denied area of interest, or turn it over to cyber experts who need it. This could be as small as a USB stick or some larger technical support equipment needed for a cyber operation. In the same way, it is also possible to exfiltrate important information devices and transfer them to a safe location for further technical investigation. The ability of SOF to operate in all extreme environments and conditions in the air, land, and maritime domains makes them particularly valuable for these kinds of operations.

In the current information era, technically trained SOF operators could integrate the so-called FRINGE technologies (photo, robo, info, nano, geno, and electro) to bridge the air gap between human and machine.¹⁷ A July 2007 Israeli raid in Syria is a good example of this kind of operation: Israeli commandos were able to infiltrate electronic warfare, cyber, and laser equipment into Syria, where they jammed a key radar station and enabled Israeli fighters carrying bombs to approach a suspected nuclear reactor site without alerting Syrian defenses. The commandos then directed the aircraft to the target using lasers, and the nuclear reactor site was completely destroyed.¹⁸

Understand, Deceive, and Influence the Cultural Environment

SOF's ability to blend in with the regional cultural environment, combined with their often unconventional operational and language skills, formidable training, adaptability, and self-reliance, make them the perfect tool to understand, deceive, and, if necessary, influence the cultural environment in foreign denied countries to prepare for cyber operations without the immediate risk of further escalation.

Building relationships, establishing human networks, and engaging with local leaders to develop community trust are some of the ways by which SOF can facilitate cyber operations.¹⁹ In the initial stages of the intrusion model, SOF can develop an understanding of the environment and set the conditions for the cyber experts to do their work. The human network of an adversary is a physical entity, regardless of whether it uses social media or other digital means to communicate, and is therefore susceptible to cross-cultural interception and influences.²⁰ SOF can exploit both physical and virtual entry points with their own capabilities, cyber means, or joint combined capabilities. These physical and virtual entry points could be exploited by cyber experts back in the home country to counter active digital hybrid threats.

Three Cyber-SOF Integration Options

Due to the scarcity of qualified technical cyber personnel in the short term, the Dutch Ministry of Defense (MoD) has started a program to hire civilian cyber specialists as reserves on a temporary basis to help with specific projects.²¹ Both the SOF and MoD cyber organizations could potentially draw on this pool of specialists when planning for operations that require specialized cyber techniques, coding, or encryption. For the longer term, there are three

options for integrating SOF and cyber capabilities: (1) delegate cyber-SOF teams to the operational commands; (2) embed SOF and cyber personnel in each other's organizations; and (3) create a new cyber-enabled special operations unit. Each option has benefits and drawbacks, and any choice the MoD makes to implement one should take into account the existing cyber and SOF organizations, leadership, and cultures.²²

Due to the scarcity of qualified technical cyber personnel, the Dutch Ministry of Defense has started to hire civilian cyber specialists as reserves to help with specific projects.

Delegate Hybrid Cyber-SOF Teams to the Operational Commands

The Army and Navy are the only two Dutch operational commands currently with SOF capabilities. The Dutch MoD, with its Special Operations Command (NLD SOCOM) in the coordinating role, could advise the two commands to set up their own hybrid cyber-SOF teams at the tactical and operational levels and integrate them into the respective Army *Korps Commando Troepen* (KCT) and Dutch Maritime Special Operations Forces (NLMARSOFF). Both KCT and NLMARSOFF could be tailored to integrate hybrid cyber-SOF teams according to the teams' anticipated needs and available resources and budget. These hybrid teams could adapt cyber expertise to the traditional MA, SR, and DA roles, while the Army and Navy SOF units could provide support to cyber operations on the tactical and operational levels.

The hybrid cyber-SOF teams would require personnel to have both technical cyber expertise and a SOF background. The operators in this team would have to be able to infiltrate a denied or hostile environment and execute various SOF tasks as required, and also be able to code, encrypt, and manipulate social media, network, and data sources using advanced tools such as FRINGE technologies.²³ Recruiting, training, and maintaining such highly skilled personnel would be challenging, but if they started small, both KCT and NLMARSOFF could experiment with cyber-SOF integration on the tactical-operational level and grow the units as they gain experience and attract qualified recruits.

If the proper mandate, legal framework, and infrastructure are in place, tactical-operational cyber capabilities can achieve significant results. In military intelligence cyber operations, for example, many activities and techniques are

already available and could be adapted for SOF-supported offensive cyber operations. In the early stages of this process, however, it might be easier to bring in private sector personnel on a project basis, or put temporary cyber enablers in SOF teams, as explained in the second option.

Embed SOF and Cyber Personnel

The second integration option is to embed SOF personnel in cyber organizations and/or vice versa. On the strategic level, Dutch SOCOM already has cyber officers liaising with DCC and JSCU, while on the operational and tactical levels, both KCT and NLMARSOFF have cyber liaisons in staff positions.²⁴ Other than these liaisons, however, there are almost no SOF planners or even operators working in the DCC or JSCU, and no cyber experts or operators are working in SOCOM, KCT, or NLMARSOFF. Beginning in 2021, however, NLD SOCOM, Dutch SOF and the DCC began participating in cyber-SOF exercises such as Crossed Swords, which was organized by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE).²⁵

The cultural understanding and situational awareness of both the SOF and cyber communities would benefit from embedding specialized personnel in each other's organizations.

The cultural understanding and situational awareness of both the SOF and cyber communities would benefit from embedding specialized personnel in each other's organizations, but doing so is complicated because of their very different institutional cultures and backgrounds. Any hope for success would depend on an extended commitment from both personnel and their organizations and leadership. The specialists would need to train, exercise, and educate one another to learn the tactics, techniques, and procedures of SOF and cyber operations. Once both sets of specialists had a basic understanding of the other's operations, they could embed in teams organized to fill future missions. A flexible mentality would be vital for every team member, because each mission demands a different approach to supporting cyber operations. Embedding personnel in this way would demand training, time, and patience to bridge the cultural gaps and foster mutual understanding.

A Cyber-Enabled Special Operations Unit

The third integration option is to create a new, centralized cyber-enabled special operations unit directly under the



strategic wings of SOCOM or DCC/JSCU. This unit could serve as the centralized authority to plan, coordinate, and prepare for cyber-SOF operations anywhere in the world.²⁶ Both KCT and NLMARSOF could benefit from this structure by integrating these teams into their exercises, training and, ultimately, operations. Depending on the structure and legal framework for an operation, the staff element of this strategic-level cyber-SOF unit could act as a sub-unified command in a supporting or supported role under SOCOM or DCC/JSCU. This dual-headed orientation would allow the staff to be both flexible and creative.²⁷ A mission set under the umbrella of one of the cyber-oriented commands demands more technical expertise than one under SOCOM, which would be more tactical in its approach. Ultimately, the legal framework for the unit itself and for its missions would determine which techniques and types of cyber operations would be allowed.

Ultimately, the legal framework for a new cyber-enabled SOF unit and for its missions would determine which techniques and types of cyber operations would be allowed.

This cyber-enabled special operations unit could, for example, undertake missions aligned with special warfare roles such as MA and SR, and DA surgical strikes. Special warfare requires cultural skills such as regional background and language ability, so that personnel are better able to blend into the local environment as needed. Although coding, encrypting, and the use of FRINGE technologies would still be important skills for the operational unit to have, special warfare is more in line with the third type of support that SOF can provide to cyber operations: to understand, deceive, and influence the cultural environment.

In contrast, surgical strike scenarios would require the cyber-enabled SOF unit to emphasize cyber techniques. These operators would have to be highly skilled in network systems and computer science, and understand the uses of FRINGE technologies in a denied or sensitive cyber domain. “These teams would perform more direct and often unilateral cyber special operations, such as crippling adversaries’ command and control (C2) systems or launching cyberattacks” to disable adversary defenses or infrastructure.²⁸ By understanding the various dynamics of MA, SR, and DA operations, cyber-SOF teams could be used across the range of SOF operations and support further cyber operations.

Dynamics, Conditions, and Obstacles to Cyber-SOF Integration

The viability of each of the three integration options will depend on several factors, including the legal framework within which it is set up, how it is financed, how well the different cultures are integrated and balanced, the command and control structure, and the quality of coordination between the groups. This list of conditions is not comprehensive and could grow longer depending on the organizational environment and political circumstances. There are, however, four critical factors that will determine the viability of the three integration options: mission impact, feasibility, professional culture, and the mitigation of possible risks. Note that it is beyond the scope of this section to compare the three integration options and draw conclusions about which might be preferable; its purpose is to discuss what steps would be necessary to adopt each one into existing MoD structures.²⁹

Critical Factors for Success

First, it is of fundamental importance to evaluate the efficiency and effectiveness of each integration option and its potential impact on mission readiness. While functional SOF and cyber teams work largely independently of one another, horizontal project teams are highly interdependent. These horizontally integrated SOF and cyber units need to develop the right functional balance between the disparate demands of their missions and workflow coordination: the rules, hierarchy, supervision, flexibility, and communication that will help to ensure that the integrated unit can meet mission requirements as efficiently and effectively as possible.³⁰ Merging cyber and SOF personnel, with their various backgrounds, education, and outlooks, into a functional unit requires choosing the integration option that will provide optimal deconfliction, coordination, and synchronization.

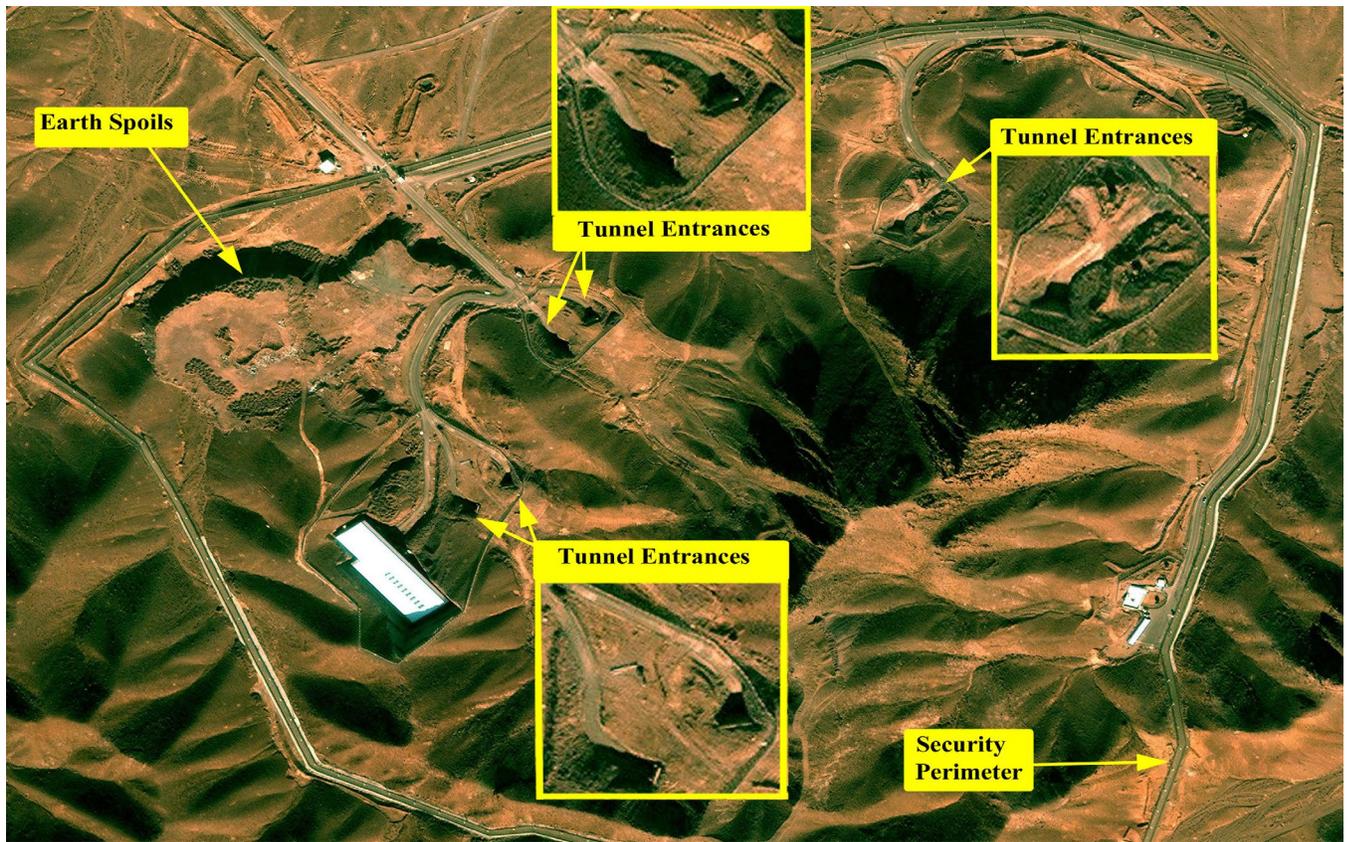
It is of fundamental importance to evaluate the efficiency and effectiveness of each integration option and its potential impact on mission readiness.

Feasibility, the second factor in choosing an integration option, requires clear measures of success: how well will the units' members be able to coordinate, cooperate, and meet their mission requirements within the institutional configurations of each option? Whether the choice of integration is a centralized, decentralized, or pooled-divisional structure, the feasibility assessment must examine both barriers and facilitators within the cultures and evaluate

the reciprocity of cyber and SOF activities.³¹ Additionally, the dynamics and conditions of the mission will influence all three options. Is a particular mission an intelligence exploitation operation under the umbrella of the security intelligence services, a special operations procedure, or an operation under the direction of SOCOM or DCC? Each role must be defined according to a specific legal framework that legitimizes the type of operation in question.

The third factor to take into account, professional culture, is less easy to define and manage. SOF and cyber personnel often come from very different cultural, educational, and training backgrounds, and these differences can have a strong effect on whether and how their units can successfully integrate.³² Strong, flexible leadership is key to bridging the cultural gaps and striking the correct balance of command, control, and coordination between the two entities.

The fourth critical consideration is risk mitigation. Lessons from the past show that the operational commands, in particular, tend to operate in a stove-piped manner, meaning that they tend to maintain their own training pipelines and particular recruiting, selection, and training criteria.³³ This stovepipe approach can result in different outcomes among the commands for similar training courses such as sniper, counterterrorism, and jungle, mountain, and arctic warfare. However, decentralizing the pipelines and delegating certain training functions, especially for cyber capabilities, might be even less efficient. The risk that stovepipe thinking affects the operational commands requires the MoD to provide strategic guidance and ensure cooperation. It is essential to break the walls around the stovepipes and integrate the various teams to mitigate the risks of a breakdown in coordination and cooperation. To gain the most significant effects through cyber warfare operations, there needs to be a central cyber-SOF structure under the umbrella of a special operations command. In the Netherlands, this would be the SOCOM, DCC, or JSCU, depending on the type of operations in question. The solution for the United States' SOCOM and CYBERCOM has been the third integration option: to build a new Cyber Special Operations Command.³⁴



Institute for Science and International Security analysis of DigitalGlobe Imagery showing the Fordow Fuel Enrichment Plant on 21 December 2013.

How the Different Cultures Can Affect Mission Readiness

A lack of reciprocal awareness and understanding can arise from cultural differences between SOF and cyber personnel, including their specialized jargon, disparate expertise, and particular planning cycles. The most important risk to overcome may be the biases that each group brings to the process of integration. It is essential to have the hearts and minds of all relevant personnel invested in the process if integration is going to be successful.³⁵ SOF and cyber operations have a symbiotic relationship at the strategic, operational, and tactical levels, but their planning processes significantly differ. Although both kinds of operations are developed, planned, and authorized at the strategic level, their execution is often at the tactical level. Tactical execution, in turn, has effects at the operational and strategic levels.

Although NLD SOCOM ostensibly uses the typical military top-down approach to give both KCT and NLMARSOF direction and guidance for planning SOF operations, in practice the process often takes more of a bottom-up approach, which is an exception in the military realm. SOF will often seek out loopholes in the planning guidance that offer opportunities to conduct operations

that may push up against legal boundaries while remaining in line with strategic intent. Cyber operations, in turn, have their own approach, which uses a version of a “spiral” planning cycle to keep up with fast-moving technology and developments.³⁶ Spiral planning is based on the intrusion model, which allows planners to accelerate or delay progress between the various steps of the planning process to meet mission requirements. (See figure 1.) For example, it can take months to develop zero-day exploits to conduct an offensive cyber operation. The model also lays out the measures the defender must take to counter an intruder and defend the cyber system.

Offensive cyber activities can be designated as special operations, just as SOF activities are, and thus fall under the same kind of approval process as other special operations.

Offensive cyber activities can be designated as special operations, just as SOF activities are, and thus fall under the same kind of approval process as other special operations; the purpose of the approval is to take into consideration any possible political and diplomatic consequences,



impacts, and effects such activities could generate.³⁷ In the Netherlands, the ministerial steering group committee on special operations was given authority to oversee offensive cyber operations executed by the DCC³⁸ prior to the start of planning.³⁹ Because of this change, both SOF and cyber operations can now be initiated, planned, and executed on every strategic, operational, and tactical level.

The first quick win for the MoD with SOCOM and the operational commands in particular, however, should be the integration of SOF and cyber experts and their capabilities in the planning process. As Commander SOCOM Major General Theo ten Haaf pointed out, “When we are looking at SOF and cyber operations, we should consider the whole process from the starting point to the end of the operation, when the evaluation is finished. Currently, we see that cyber is integrated too late into the planning process.”⁴⁰ This cyber-SOF integration also means learning from one another, as Commander DCC Commodore Boekholt O’Sullivan described: “SOCOM is short-term focused, while DCC is more oriented on a longer period. SOF personnel need to slow down in their decision-making versus DCC, which could learn to accelerate in their process or at least urge SOF to slow down.”⁴¹

Common Institutional Hurdles to SOF-Cyber Integration

The Netherlands has the cyber tools it needs to effectively counter domestic or international hybrid threats, but it still lacks a clear legal mandate for cyber operations at the level of national security. This is a common problem, especially with offensive cyber operations in the military realm. Dutch government agencies in general, including the MoD, are not sufficiently knowledgeable about the uses and possibilities of cyber technologies. Despite current initiatives to position military cyber liaison officers, the MoD still lacks direction and planning from leadership and a clear vision of how to integrate cyber tools into military operations.⁴² Cyber assets should be seen as an integral part of every military planning process; more than that, they are the “satay skewer” connecting all the various layers of an operation.

The Dutch MoD still lacks direction and planning from leadership and a clear vision of how to integrate cyber tools into military operations.

The same is true for cyber personnel policy: the MoD has inadequate career paths for cyber experts, and it lacks a clear cyber personnel policy.⁴³ An effective policy would be to create specific career paths in infantry, intelligence, SOF, and signals to allow cyber specialists to incorporate new functions and develop expertise throughout their military careers. Furthermore, the financial incentives are disproportionate: a cyber expert can make much more money in the private sector than by working for the government, which makes it very difficult for the MoD to keep the most talented cyber experts onboard.

A third obstacle is the fact that senior leaders in the Dutch MoD generally have little experience in the cyber domain, and limited “cyber awareness”—knowledge of current technologies, applications, developments, and the knowhow to implement them—which results in a narrow concept of command and control in the cyber realm. Cyber illiteracy among senior military decision makers also creates gaps and inefficiencies in the use of available cyber technologies. Stovepipe thinking, traditional mindsets, and the lack of personal cyber experience lead to functional biases and, often, a refusal to accept that the virtual landscape has changed beyond the individual’s understanding. In civilian tech firms, an effective boss will listen to his or her cyber experts and use their knowledge and advice to inform decision-making, while in a governmental organization like the MoD, the person with the highest rank makes the decisions, including whether to listen to subordinates’ advice.⁴⁴ Without a broader joint military and inter-agency government approach, the Netherlands will continue to miss opportunities to counter the hybrid threats the country faces.⁴⁵

The Way Ahead

This article has laid out three potential roles that SOF could play in support of cyber operations; the choice of which one to adopt depends on the effects and end states that the MoD wants to achieve. It is also important to keep in mind that the conditions in the operation area may not be conducive to every supporting role. How to successfully integrate cyber and SOF units on the other hand, requires understanding the strengths, weaknesses, and cultural gaps between SOF and cyber personnel and their organizations. Both SOF and cyber capabilities are scarce, precious, and effective national strategic assets, which NATO countries are not often willing to share. Therefore, any effort to integrate the SOF and cyber personnel of NATO members in support of NATO cyber operations will be an even more ambitious and long-term process.

To begin this effort, the C-SOCC gave Belgium, Denmark, and the Netherlands the opportunity in 2021 to experiment with and practice the integration of SOF and cyber capabilities. So far, this tri-national experiment has only produced some basic lessons learned during Exercise Night Hawk that might be useful for other NATO SOF and cyber countries.⁴⁶ For future SOF and cyber missions, C-SOCC could become the foundation of a NATO composite command integrating SOF and cyber capabilities. Even so, national caveats, mutual trust, and a proper legal framework are keys for successful SOF and cyber integration and to smooth the process of cooperation. However, NATO’s new regional SOCC focus and the possibility of establishing Regional Special Operations Component Commands (R-SOCC) have the potential to radically enhance cooperation among geographically neighboring NATO countries with SOF capabilities.⁴⁷

National caveats, mutual trust, and a proper legal framework are keys for successful SOF and cyber integration and to smooth the process of cooperation.

On the national level, political-strategic leaders inside the Dutch MoD are not doing enough to create an environment that is conducive to SOF and cyber capability integration. During an interview with the author, former Director Joint SIGINT Cyber Unit Marc Brinkman explained: “The political military-strategic level should set up a research and development environment where SOF and cyber could experiment, facilitate, test, develop, and innovate to create the right conditions to set SOF-cyber integration up for success.”⁴⁸ In short, the senior MoD leadership should create the conditions that promote better and deeper integration between SOF and cyber capabilities by establishing a clear directive with national guidance. MoD leadership need not search for the solutions, but can instead create the fertile conditions and simply listen to their SOF and cyber specialists to promote SOF and cyber integration, synchronization, and cooperation.

ABOUT THE AUTHOR

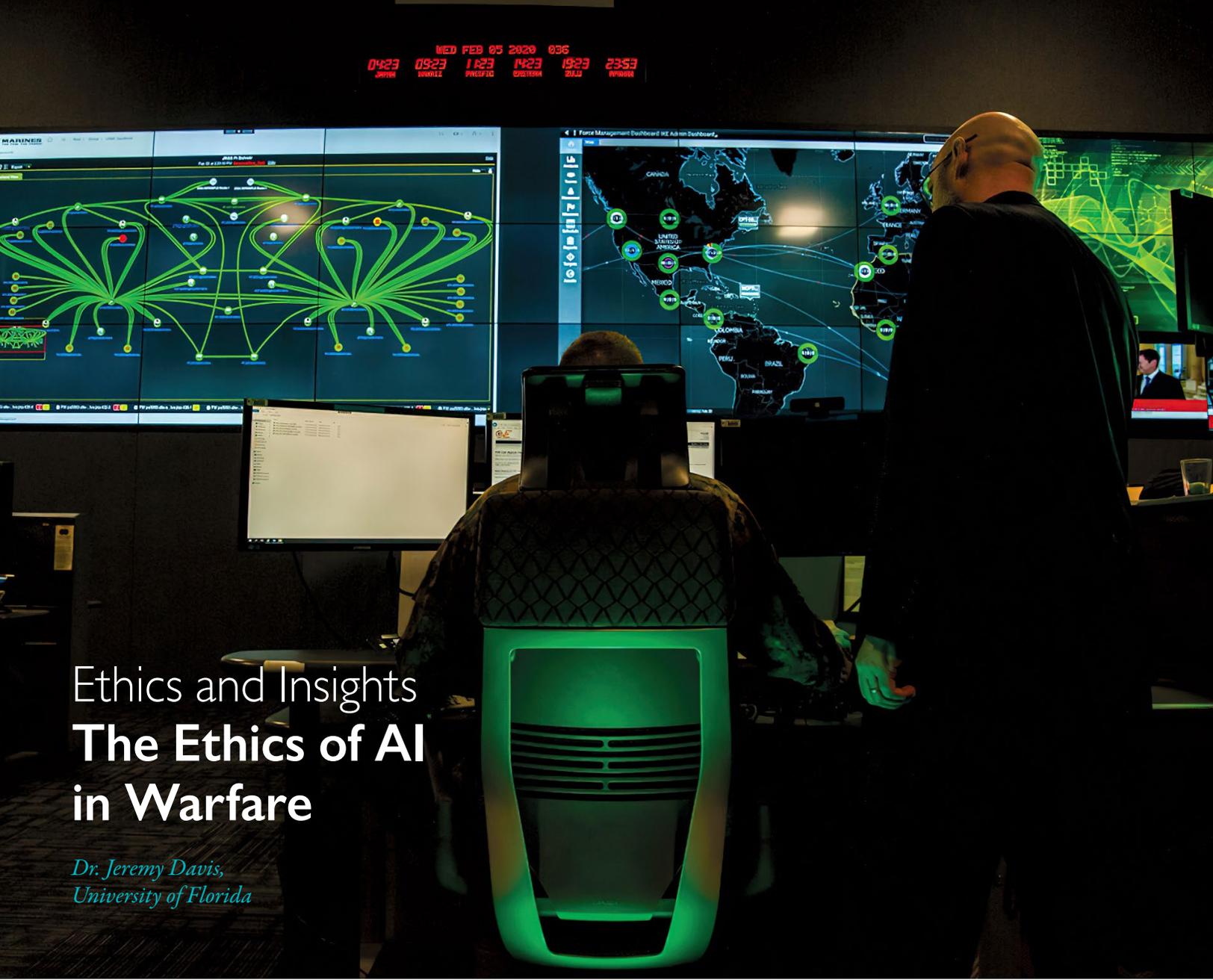
LTC Jonas van Hooren serves as a staff officer in the Netherlands Ministry of Defense.

This is a work of the US federal government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

NOTES

1. According to the Dutch Defence Cyber Strategy 2019, digital warfare is defined as any activity involving the use of computer code or data stream to achieve military objectives.
2. This article was derived from the author's master's thesis: Jonas van Hooren, "The Imperative Symbiotic Relationship Between SOF and Cyber: How Dutch Special Operation Forces can Support Cyber Operations" (master's thesis, Naval Postgraduate School, 2019): <https://calhoun.nps.edu/discover?query=van+hooren>. Unless otherwise noted, all translations from Dutch to English are by the author.
3. "Composite Special Operations Component Command Reaches Full Operational Capability," NATO, 20 May 2021: http://www.nato.int/cps/en/natohq/news_179986.htm
4. "Zero Days: VPRO Tegenlicht," 12 October 2014, YouTube, video, 49:16: <https://www.youtube.com/watch?v=JhkXSg9KQE8>
5. National Coordinator for Security and Counterterrorism, *Xiμαρα: An Analysis of the "Hybrid Threat" Phenomenon* (The Hague: Ministry of Justice and Security, 2019), 9: <https://english.nctv.nl/themes/state-threats/documents/publications/2019/09/05/analysis-of-the-'hybrid-threat'-phenomenon>
6. William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (New York: Presidio Press, 1996).
7. NATO, AJP-3.5, *Allied Joint Doctrine for Special Operations* (Brussels: NATO, 2013).
8. Colin S. Gray, *Explorations in Strategy* (Westport, CT: Greenwood Press, 1996), 145.
9. Ibid.
10. While interviewing sources, the author was told various first- and second-hand examples of classified operations where SOF were used as the initial entry force to pave the way for cyber operations.
11. Tactical Sight Exploitation (TSE) is a task SOF personnel normally conduct after clearing an area or building to search for fingerprints, signs, or (digital) evidence that will assist prosecution.
12. Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (New York: Oxford University Press, 2017), 33: <https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012>
13. "USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers," 28 January 2016, YouTube, video, 34:55: <https://www.youtube.com/watch?v=bDJb8WOJYdA>
14. "Cyber Security: Understanding the 5 Phases of Intrusion," Graylog (blog), 26 August 2020: <https://www.graylog.org/post/cyber-security-understanding-the-5-phases-of-intrusion>
15. Classified documents provided by former NSA employee Edward Snowden and reported by the *New York Times* in 2013 prove this technique. See Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, 5 September 2013.
16. David E. Sanger and Thom Shanker, "N.S.A. Devises Radio Pathway into Computers," *New York Times*, 14 January 2014: <https://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?searchResultPosition=1>
17. Patrick Duggan, "SOF's Cyber FRINGE," *Small Wars Journal*, 10 February 2016: <https://smallwarsjournal.com/jrnl/art/sof%E2%80%99s-cyber-fringe>
18. Eric Follath and Holger Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor," trans. Christopher Sultan, *Der Spiegel International*, 2 November 2009: <https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html>
19. Jessica Glick Turnley, *Cross-Cultural Competence and Small Groups: Why SOF Are the Way SOF Are*, JSOU Report 11-1 (MacDill Air Force Base, FL: JSOU Press, 2011), 13: [https://www.soc.mil/528th/PDFs/JSOU11-1turnleyF-DWDandSmallGroups\(Turnley\)_final\(16Mar\).pdf](https://www.soc.mil/528th/PDFs/JSOU11-1turnleyF-DWDandSmallGroups(Turnley)_final(16Mar).pdf)
20. Patrick M. Duggan, "U.S. Special Operations Forces in Cyberspace," *Cyber Defense Review* 1, no. 2 (2016): 73-79.
21. Commodore Boekholt O'Sullivan (Commander Dutch DCC), interview with the author, 10 September 2019.
22. From 9 to 11 September 2019, the author conducted interviews in the Netherlands with SOF and cyber specialists to hear their opinions on the viability of the cyber-SOF integration options.
23. Duggan, "SOF's Cyber FRINGE."
24. Commanders NLD SOCOM and Dutch DCC, interviews with the author, 9-10 September 2019.
25. "Exercise Crossed Swords 2020 Reached New Levels of Multinational and Interdisciplinary Cooperation," NATO Cooperative Cyber Defence Centre of Excellence, n.d.: <https://cccoe.org/news/2020/exercise-crossed-swords-2020-reached-new-levels-of-multinational-and-interdisciplinary-cooperation/>
26. Benjamin Brown, "Expanding the Menu: The Case for CYBERSOC," *Small Wars Journal*, 5 January 2018: <https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc>
27. In interviews with Commanders NLD SOCOM and Dutch DCC, both commanders stressed the importance of a flexible and creative mindset within cyber-SOF operations, where the command relationship is supporting or supported. Interviews with the author, 9-10 September 2019.
28. Brown, "Expanding the Menu."
29. It is important to keep in mind that these recommendations are based on the Dutch MoD, and thus are not intended to be a template for other defense organizations, which will need to evaluate their own institutional, structural, and cultural conditions before making decisions.
30. Richard L. Daft, Jonathan Murphy, and Hugh Willmott, *Organization Theory and Design* (Andover, UK: Cengage Learning EMEA, 2014), 277.

31. James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (Piscataway, NJ: Transaction Publishers, 2003).
32. In interviews, both Commander NLD SOCOM and Commander Dutch DCC mentioned that differences in culture and the need for mutual understanding between SOF and cyber personnel are the primary foci for a successful integration. Interviews with the author, 9-10 September 2019.
33. Commander NLMARSOF has no issues with NLMARSOF having its own courses. However, cyber integration needs to be coordinated from the strategic level for both NLMARSOF and KCT. Conference call with Commander NLMARSOF, 26 September 2019.
34. Brown, "Expanding the Menu."
35. O'Sullivan, interview.
36. Cyber expert Jelle Haaster and FOX-IT encryption manager Daniel Datau explained the differences between conventional SOF planning and the spiral cyber planning. Interviews with the author, 10-11 September 2019.
37. A.Th.B. Bijleveld-Schouten, "Vaststelling van de begrotingsstaten van het Ministerie van Defensie voor het jaar 2018 ; Brief regering; Reactie op verzoek commissie om inzicht in besluitvormings- en verantwoordingsproces inzake speciale en geheime operaties," officiële publicatie, Staten-Generaal der Tweede Kamer, [Determination of the Ministry of Defense Budget Statements for the Year 2018; Government Letter; Response to Committee's Request for Insight into Decision-Making and Accountability Process regarding Special and Secret Operations, Official Publication States General of the Second Chamber], 27 March 2018: <https://zoek.officielebekendmakingen.nl/kst-34775-X-88.html>
38. O'Sullivan, interview.
39. Paul Ducheine and Kraesten Arnold, "Besluitvorming Bij Cyberoperaties" [Cyber-Operations Decision-Making], *Militaire Spectator*, 20 February 2015: <https://www.militairespectator.nl/thema/recht-cyberoperaties/artikel/besluitvorming-bij-cyberoperaties>
40. Major General Theo ten Haaf, Commander NLD SOCOM, interview with the author, 9 September 2019.
41. O'Sullivan, interview.
42. Interviews with Commanders NLD SOCOM, DCC, JSCU, KCT, and NLMARSOF. All commanders agreed that the role of liaison officers between SOF and cyber is crucial. Interviews with the author, 9-11 September 2019.
43. Interviews with Commanders Dutch DCC and JSCU. Both DCC and JSCU commanders agreed that recruiting and keeping the educated and experienced cyber personnel in-house are real challenges. Interviews with the author, 10 September 2019.
44. Huib Modderkolk, *Het is Oorlog maar Niemand die het Ziet* [There's a War Going On, But No One Can See It] (Amsterdam: Publisher Podium, 2019), 39.
45. Commander JSCU, interview.
46. "NSPA Supports Exercise NightHawk in Denmark," NATO Support and Procurement Agency, 1 October 2021: <https://www.nspa.nato.int/news/2021/nspa-supports-exercise-nighthawk-in-denmark>
47. "Multinational Capability Cooperation," NATO, 2 February 2022: https://www.nato.int/cps/en/natohq/topics_163289.htm
48. Marc Brinkman, former director, Joint SIGINT Cyber Unit, interview with the author, 9 September 2019.



Ethics and Insights The Ethics of AI in Warfare

*Dr. Jeremy Davis,
University of Florida*

PROFESSOR BRADLEY J. STRAWSER OF THE US Naval Postgraduate School (NPS) invited Dr. Jeremy Davis to address students in the Defense Analysis department on the ethical implications of using artificial intelligence in combat operations. Dr. Davis’s primary research explores questions of normative and applied ethics, particularly with regard to war and policing. The lecture took place at NPS on 27 September 2021.

BRADLEY STRAWSER: There aren’t many scholars and philosophers who do work on military-related ethics, and so we are lucky to have Dr. Jeremy Davis speak to us today. After his lecture, we’ll have an open discussion, and we’ll be using Chatham House rules, so there will be no attribution of any of the comments or questions.

JEREMY DAVIS: Today, I’d like to address a big question that I think philosophers, ethicists, and maybe even folks

in the military spend too little time thinking about, and that is the role of algorithms in justifying killing. I’m particularly interested in hearing what service members have to say about this topic; I’m not a service member, and I know that you have a keen eye and a distinctive perspective on this topic, so I’m serious about hearing your thoughts. I’m going to set up a strict account of the issues, and if it’s wrong, you tell me why.

Project Maven and Artificial Intelligence in War

Project Maven, also known as the US Department of Defense Algorithmic Warfare Cross-Functional Team, was instituted in April 2017. Its aim was “to accelerate DoD’s integration of big data and machine learning” in order to “turn the enormous volume of data available to DoD into actionable intelligence and insights at speed.”¹ More

specifically, the initial phase of the project was to create, train, and ultimately deploy machine-learning technology to sift through the countless hours of data that have been collected through the military's various surveillance methods. I'm going to talk today about how that's gone awry in some cases.

Project Maven was instituted in April 2017 “to accelerate DoD’s integration of big data and machine learning.”

One of the more obvious reasons for something like Project Maven is to respond to a number of inefficiencies that present themselves when one is dealing with massive swaths of data. The first problem is that there's just far more data being collected than humans can process. According to one calculation, the Air Force alone had acquired so much surveillance footage in Iraq over the course of a single year that it would take one person 24 years of working nonstop to get through it all. According to another estimate, 700,000 hours—that's 80 years—of footage was collected in 2017 alone, so obviously, there's far more data than even teams of observers could realistically deal with. Second, a lot of the data that are generated are completely useless, so spending countless analyst-hours on that is a massive waste of resources. Finally, it's really difficult to draw connections across data and be able to identify the source of problems or potential leads to follow up on if you have multiple massive teams of people working, particularly teams that aren't necessarily speaking with each other or even focused on the same set of issues.

A lot of these inefficiencies or challenges can be resolved by shifting to big-data methods—machine learning—where you can create algorithms, create systems, in which a lot of these inefficiencies can be completely eliminated. The systems can identify connections; they can sift through countless hours much better than enormous teams of potentially sleepy or bored people watching cameras all day. Machines solve that problem. Of course, the ultimate goal is not only to solve that problem, but also to create a lot of strategic advantages as well.

Although a lot of information about Project Maven is classified, the topic of artificial intelligence (AI) in warfighting has come to the public's attention in the past few years, and there has been some discussion of it in public venues. A civilian might have first learned about Maven when Google decided that it wasn't going to renew its contract with the Pentagon. Many of its AI researchers said they didn't want to have anything to do with the project. A number of

other companies then stepped in to fill the void, including Anduril, Clarifai, and Palantir. The last of these is probably the most widely known to you, because Palantir is one of the developers of predictive policing technologies.

Project Maven is one of the many different programs within DoD to advance AI. We're not really talking here about the killer robots phenomenon, but I'll say more about that in a minute. We're talking specifically about the use of algorithms in developing technologies that humans ultimately will be responsible for using. There's also a program called Atlas, which stands for Advanced Targeting and Lethality Automated System. I've got a quote from an Army engineer about how the algorithm isn't making the judgment—and here we need to draw a contrast with killer robots. We're not just setting this thing free to do whatever it wants; the algorithm is providing information to aid the service member in deciding what to do. There's also been some preliminary research into outfitting tanks with AI weapons, which is going to involve machine-learning algorithms that will help not only to identify people who are known to us as targets, but also to make predictions about where people will go, what they are doing, what they're going to do, whether or not the action that we see them doing constitutes a threat, and that sort of thing.

For the sake of definition, we're going to call these “algorithmic systems.” We are talking about something that relies on big data, algorithmic processing, and/or machine learning: typically, all three. It is both historical and predictive; it both takes facts that we already have about a person, such as biometric data or whatever, and also makes predictions about where they're going to be and what they're going to do, and so aids us in making decisions. It can be used particularly in the military context, although it does have a broader range of applications.

We are talking about something that relies on big data, algorithmic processing, and/or machine learning: typically, all three.

As I said earlier, I think philosophers and ethicists have spent far too little time thinking about this. They're fixated instead on the phenomenon of extreme killer robots that we'll set free to do all of our bidding. We're much further away from those than we are from these data systems, which are being developed and exist now. We need to ask actual questions that apply to these systems, particularly because, as with most technologies that are already being used, we didn't ask these questions *before* they were put into use, right?



Airman 1st Class Sandra, 7th Intelligence Squadron, explains how Project Maven works at a booth during the 70th Intelligence, Surveillance and Reconnaissance Wing's 2018 Innovation Summit 24 July 2018 at College Park, Maryland.

The Man in the Purple Hat

I want to tell you a story. This is the story of the Man in the Purple Hat. It's from the book *First Platoon* by Annie Jacobsen, who's a celebrated journalist.² The story takes place in Afghanistan and centers on the Persistent Ground Surveillance System, or PGSS. It happened in 2012, several years before Project Maven was instituted, so the system was kind of a precursor, and it alerts us to the problems that are latent in these systems. PGSS is basically an enormous blimp, and one of the things it does is to take 24/7 surveillance footage of all the areas relevant to its instructions, and then organizes, processes, and tags the footage using software that was developed by Palantir. The technology helps the military track particular individuals. It's not really predictive; it's just tracking. It's meant to understand individual habits, to identify them and to say, look, here's where they tend to go. As it acquires this data about people, it will be able to make predictions, but it's primarily used as an identification tool.

A man named Kevin is the PGSS operator at the time the story takes place, and he's monitoring a man in a purple hat. From many hours of surveillance, Kevin comes to believe that the Man in the Purple Hat plants IEDs in an effort to harm civilians or soldiers. Once Kevin compiles

enough evidence, he takes it and runs it through Palantir software, which enables him to keep a closer eye on the Man in the Purple Hat, and even to predict where he's going to be. Kevin's unit designates the man with a "429 package," meaning that when the time is right, they're going to take him out. They think this is a bad guy, and it's his time. One day, Kevin's colleagues inform him that they have the Man in the Purple Hat in their sights, and they think it's time to call in air support and take him out. Kevin's colleague points the man out on the screen, and Kevin notices that he's sitting on a tractor. After a few minutes, with air support on the way, Kevin starts having second thoughts. He later told Annie Jacobsen, "I thought, wow, that looks like him, but something just gave me a tickle that it wasn't him. Number 1, he's not a worker. He's a bad guy, and bad guys don't tool around on tractors and play farmer. I said, 'I'm certain it's not him.'" His supervisor says, "Well, you've got five minutes to figure that out and prove me wrong." So Kevin runs over to the Tactical Operations Center—he literally runs over there—to prove that it is the wrong man. He has the operator inspect the home of the Man in the Purple Hat, and sure enough, the man they are looking for is actually at his home.

This was a case of mistaken identity. Fortunately, they called off the strike. According to Kevin, had a computer

done the algorithm on the guy on the tractor, as far as the computer was concerned, that was him: the Man in the Purple Hat. But because Kevin had been watching him for months, he knew that it wasn't him. "I knew his face. I doubted the computer. I was right."

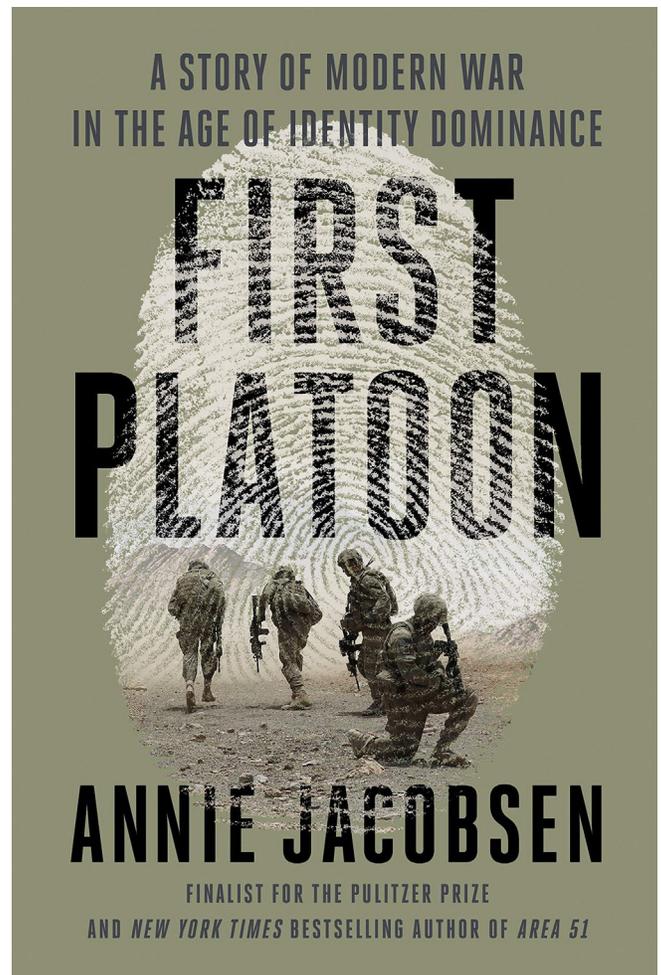
As far as the computer was concerned, that was him: the Man in the Purple Hat. But because Kevin had been watching him for months, he knew that it wasn't him.

That story is probably a familiar story to service members and may be kind of unremarkable to many of you. But to a civilian like myself, that story blows my mind, because we got *that close* to killing a completely innocent farmer. I know this stuff happens all the time. But hearing it in those details, especially from the perspective of the guy who had a gut feeling that he was right and he was correct about that, is really interesting. It draws that contrast between what the algorithm told us and what the humans with their instincts and perspective said. Again, this is a case of mistaken identity, but the algorithms are also likely to make errors concerning threats when they're dealing specifically with predictive elements, such as whether somebody who's holding something is holding a gun, or another weapon, or maybe just some farm tool, or something else. And, you know, this constitutes the full range of things that might be viewed as evidence that could justify killing someone on the basis of what ultimately turns out to be some kind of algorithmic error. Now this case had a relatively happy ending, but there are no doubt other cases in which that wasn't the result. We certainly know that from drone cases, and we have no reason to believe that errors won't happen commonly with respect to these algorithmic systems as well.

Predictive Killing

The story of the Man in the Purple Hat calls to mind a number of distinctive ethical questions. The one I want to focus on is the role that algorithms can play in justifying killing. I mean this in the ethical sense. I'm not talking about what passes the relevant codes or restrictions that might be placed upon you in your distinctive roles, or what you can get away with in the legal sense, but ethically, what can justify using these algorithms to make decisions about killing?

I'm going to highlight just a few basic issues here about whether these things can justify killing. The first question to ask is, well, what evidence do they offer us? What is their evidentiary value? There's a basic question here about whether the various statistical inferences at work within



these algorithms can count as evidence at all. I think the answer has to be yes, it counts *somewhat*. To the extent that it's decisive is a separate issue, but it certainly does seem to count more than, for example, a Ouija board.³ I think that, for obvious reasons, it would be pretty shocking if we were just relying on the evidence provided by a Ouija board. The question, it seems to me, is not whether information from an AI device could, in principle, count as evidence, but whether the algorithms, such as they are, provide *sufficient* evidence in the context in which they are used, for the types of things they're expected to justify. So we don't just want to say, look, they provide evidence; they tell us information we didn't already have. We know that. The question isn't whether they tell us something we didn't already know. The question is whether they tell us *enough* to be able to justify what it is we're using them for. I think that's the important ethical question.

The question isn't whether they tell us something we didn't already know. The question is whether they tell us enough to be able to justify what it is we're using them for.

As in most algorithmic systems, the ones we're talking about are fundamentally opaque. That's a kind of technical term, even though the words are not technical. These systems are opaque in the sense that even those who use them couldn't explain why the algorithms have come to the conclusions that they have. In this sense, they are like a Ouija board. You don't know why you ended up on these letters; you just know that you did. Whereas with human deliberation, you can say, "Oh, explain that again to me; I didn't quite get that," with a lot of these algorithms, you just get, "That's the answer. That's the guy." It doesn't explain to you why, or give you all the data points that yielded that conclusion. In fact, in many cases, it cannot do that, even on the best version of the algorithms. Moreover, the systems are prone to mistakes from bad input data. You get cases where it's just terrible data that gets filtered through, and in many cases, you don't know that the data is so bad until it's too late. If Kevin's unit *had* killed the Man in the Purple Hat, we wouldn't necessarily have known which data points gave us that conclusion. Incidentally, in her book, Jacobsen says they think that the system identified the wrong man because of the way that the light hit his hat. They think that the man on the tractor was actually wearing a blue hat and the cameras weren't sophisticated enough to pick up that difference because of the differences in lighting between rural Afghanistan and whichever locations were within the system's data set, which is scary.

So that's just about identification issues. With predictive issues, we're trying to make predictions about what people will do, and it's really hard to do that. We're very bad at predicting what people will do. Algorithms are also very bad at predicting what people will do. This is true with predictive policing systems as well. We can make highly informed guesses. But again, we're not just talking about whether we should keep a closer eye on a certain person. We're asking whether this prediction gives us something like a justification for killing them, or potentially targeting them, right? So there really is a separate issue here about whether we can say, look, we think he's going to go into that area, and whether he will actually do that. That's an important issue when we look more broadly at the predictive versions of these technologies.

There are reasons to be skeptical about the accuracy of the entire system. It's all classified. It's not subject to audit. By contrast, predictive policing systems can be audited. Predictive policing systems allow police departments to make predictions about things like which areas are going to have higher crime or which individuals are more likely to commit crimes, and the police can target their resources to those areas or those people on the basis of that algorithmic prediction. The algorithms in predictive policing systems can be subjected to an audit, in which an external supervisor comes in and explores the data. This happens all the time. In fact, there are companies whose entire mission is just to do these kinds of audits. In contrast, it seems highly unlikely that the US government is going to give an outside third party access to its treasure trove of data in order for that third party to say whether or not these systems are good. An audit could be done internally, but the public at least is going to be skeptical of that kind of audit and its ability to reveal what we want to know.

Suppose the algorithm recommends killing someone who is, in fact, innocent, and a soldier carries out the killing. Unless there's abundant evidence that emerges after the fact that this person was actually innocent, the algorithm and those who rely on it will inevitably see this and code it as a successful kill. If they had killed the Man in the Purple Hat, we would have had no reason to say that they made a mistake. Maybe later, we would get some information about that, but I'm not super confident that someone's going to say, "Oh, we found that out. Let's go adjust the algorithm." What seems more likely is that it's not going to be something we'd want to admit to or embed in the algorithm. Ideally, we do, but even in those cases, we'd have to have that additional information to be able to do that.

If the initial data and the secondary and ongoing data collection process are corrupted, they're just going to keep replicating those problems to an exponential degree.

So it seems to me that, in a way that's almost unique to this particular domain of algorithms, we're much *less* likely to have accurate data. That's not just a problem: that error compounds, because the whole point of these systems is that they take data and make inferences on the basis of it over time in an iterative way. If the initial data and the secondary and ongoing data collection process are corrupted, they're just going to keep replicating those problems to an exponential degree. This is a huge problem. If you have a software program that makes predictive texts on your

phone, and you tell it, “No, that’s not what I wanted,” it will say, “Okay, thanks,” and it can make corrections. But if you never tell it, “No, that’s not what I wanted,” it’s going to keep doing what it thought was good, and it’s going to think it’s getting it right.

My concern is not just that these algorithms are bad, it’s that they’re going to continue to get worse and worse if we don’t have a system for stopping them—and I don’t think we have a system for stopping them. We know they’re imperfect. We don’t know how imperfect. We don’t have the ability to assess their imperfections. We do think, however, that there is a positive non-zero evidentiary value. It’s not just a Ouija board; it’s doing something that, at least broadly, is pointing us in the right direction. It’s also going to give us justifications—at least in the minds of some—to do things that we want to be very careful about.

We’re talking about what kind of justification we’re interested in. Philosophers sometimes like to draw a distinction between fact-relative justifications and evidence-relative justifications, and I think this distinction is going to be an important part of this discussion. So, fact-relative justification simply asks, was the target actually guilty? Was he *actually doing* the thing we thought he was going to do? This concerns a fact-relative justification. But you can imagine a case in which we get it wrong, and we say, “Hey, look, the best possible evidence we had told us that he was going to kill us.” We might think that this doesn’t make killing him right in a *fact*-relative sense, but we might speak of it as being *evidence*-relatively justified. In other words, maybe you shouldn’t be blamed for killing him. Maybe your decision should be investigated, but you shouldn’t be held to account for it. You acted on the best possible evidence, so the outcome can be justified in light of the evidence, even if it’s not objectively right, or even if it’s not fact-relatively justified. Often, we’re not going to know, and what we’re really interested in is whether, when that algorithm says “kill,” we can kill and be justified. I think this question is our quarry.

Take the case of the Man in the Purple Hat. Would it have been evidence-relatively justified to kill the farmer who might be the Man in the Purple Hat? I’m not sure. I think probably not, for some complicated reasons relative to the story, as well: obviously, Kevin had doubts. That’s enough to question the evidence, but would somebody else in his place, who didn’t have those specific doubts, have been justified? I’m not so sure. I’m curious to hear your thoughts.

If there’s an evidence-relative justification we need to be concerned with, what is the threshold for having enough evidence?

Another point here is, what is the right evidentiary threshold? If there’s an evidence-relative justification we need to be concerned with, what is the threshold for having enough evidence? Here’s a view that I want to pitch to you, and you tell me whether you think it’s wrong or you think it’s right. This is what I would call the strong view. It’s the stubborn, recalcitrant, strong view that’s very *not permissive*: predictive algorithmic systems of the sort we’re talking about generate insufficient evidence for an evidence-relative justification to kill. Why? Because the justificatory threshold, the evidentiary threshold for killing is super, super high. In order to justify killing someone, we need more than just a computer telling us that that’s the guy, and he’s going to kill somebody. If you’ve seen the movie *Minority Report*, you’re familiar with the problem here.⁴ So this is what I call the strong view: you can’t do it. It’s not evidence-relatively justified. It might be fact-relatively justified. It might turn out that the target actually *was* the bad guy. But our evidence didn’t give us enough information to be able to draw that conclusion. Our evidence was insufficient. That’s the point that I’m pushing on this class today, and I want you to push back against me and tell me if and why you think that’s wrong.

As I said, the evidence that’s generated by the technology is insufficient to meet that threshold. Here’s a set of thresholds that you might endorse. Now, these thresholds are about liability, but you might think of them as evidence thresholds as well. Michael Zimmerman is a philosopher; Adil Haque is a legal scholar; and the other—you might recognize the guy—is Barack Obama. Actually, the Obama administration’s threshold is the most restrictive and I think it’s closest to what I would be inclined to endorse: we would need *near-certainty* that the target is present, and that there would be no noncombatant collateral deaths. Adil Haque, who is a legal scholar at Rutgers, thinks that with liability, we need evidence that it’s *more likely than not* that the target is liable. Michael Zimmerman says that it has to be *likely enough* that the person is liable. That seems to me vague, because we want to know how likely is likely enough. It kind of kicks the can down the road a bit. As for more likely than not—50 plus 1—that seems too low to me, frankly. Near-certainty is what I’m going for. I want a threshold that’s quite high.



The MQ-1B Predator UAV

STRAWSER: Jeremy, just thinking through these epistemic standards, it's a fascinating thought experiment you're setting up here. But if you're not sure how you feel about these standards, one thing I encourage people to do is to consider the basic philosophical reflection of reciprocity. Which one of these standards would you want an adversary to apply to *you*? I would want it to be right!

DAVIS: Ask what you could justify to someone else. If you were speaking to the family after you killed their brother, and said, "Look, it was a 50:50 shot and, like, 50-plus; we were right there," they'd say, "No, you killed him." Again, these decisions are based on algorithmic systems, and are typically being made by people who are far removed from the action. This also involves the question of necessity. In addition to the evidence of whether or not we can justify killing him, we need to answer other morally relevant questions as well. One of these questions is whether it's necessary to kill him *now*. Think about the Man in the Purple Hat. It was not necessary to kill him at that moment. They could have waited. In fact, they did wait, and it was fine, right? But what if he were a serious target who was about to do something horrible? Even so, there was no evidence that, right then, when he was sitting on the tractor taking a nap, he was going to do something awful. He didn't have any kind of trigger or anything in his hand, right? So

based on necessity or last resort, which is a condition that you're all familiar with in the law of armed conflict, or in the conditions of *jus in bello*—the conditions that apply to soldiers in war—it doesn't seem like we passed that test, so that's going to challenge justification as well.

It's not just a matter of whether you have enough evidence; it's also a matter of whether all the relevant moral conditions are satisfied. Just to give you a sense of what I'm after here, you might also think about whether there are other less harmful alternatives that are available. The algorithm says, "This is our guy." But maybe we need to gather further evidence from alternative sources that aren't the same algorithm. Unfortunately, we might have to expose some of our service members to the risk of getting harmed in order to confirm the algorithm. Or we could apprehend the subject rather than killing him, right? Those are reversible approaches that involve satisfying our moral constraints and not potentially killing innocent people.

There's a question here that's not just about the specific instance. We want to zoom out a little bit. We can look at the case of the Man in the Purple Hat or this other thought experiment, and we might ask whether it was justified. Is the practice of relying on these systems justified? Is the practice itself justified? Is it evidence-relatively justified

to institute the practice of relying on these systems in a military context? Again, these are points I've already made. We have unreliable evidence. In fact, I think we have really good reasons to believe that the evidence is bad—better than human evidence in some cases, but potentially corrupted in ways that, again, risk that it's just going to be replicated over time. Given that we know this, we might say that the practice of using these to justify killing is specious. There's a whole other talk we could have about this: the risk of over-reliance, the resort to using this method rather than all these alternatives . . . People who are skeptical of the usage of drones will make the same point: they'll say, look, in isolated incidents it is particularly valuable, but they might worry that reliance on this system, on the whole, generates problems that wouldn't be there if we were more cautious about its use.

Is it evidence-relatively justified to institute the practice of relying on these systems in a military context?

There's a concern here, too, that this might entrench our attitudes against putting people in harm's way, which is good—I don't want any of you to be harmed—but allowing for that to be further entrenched in our attitudes will keep us at a distance from the kinds of acts that we're committing, and will make us more likely to rely on automated systems for reasons that are meant to keep the public happy and that sort of thing.

I'll pause here now to get a sense of what you think about this. I love to have disagreements. If you think I'm dead wrong, you can tell me I'm dead wrong and tell me the reasons why. I won't be offended.

SPEAKER 1: We were talking earlier about the development of the algorithms for self-driving cars, and how right now, in that experimental phase, we need to just accept some risk to develop those algorithms. So, looking at the scenarios you've presented here, and knowing that the United States is not the only competitor developing this type of stuff, we do have the highest ethical standards that we have to apply to it—hence this entire discussion. But our adversaries don't have those same standards, at least to my understanding. They're going to accept a lot more risk, so I think, looking at this situation holistically, we need to accept that same level of risk, so that whenever we enter into an actual shooting war with those competitors, we're not behind them. The systems that are being developed could potentially save far more lives than are being mistakenly struck now based on those algorithms. So, not to be

callous, but looking at the greater good, couldn't a few bad strikes resulting in civilian casualties now potentially save a brigade from destruction 20 years from now?

DAVIS: I think this question relies on some empirical assumptions that I'm not sure about. Is it true that our using this software now is going to be important for us to beat our adversaries? Why not have the systems developed and run them alongside what we're doing, but not use them to try to justify killing? For example, in predictive policing, you can run these systems and say, "We think that guy's going to kill somebody. Oh, interesting! He didn't kill anybody. Okay, the algorithm was wrong. Let's recalibrate it. We know the world turned out this way. He didn't actually kill someone." It's like you're playing computer simulations of games before they happen. There's a sports blog that actually does this: it runs Madden simulations before every game and predicts how things are going to go. They're not actually doing anything, right? It's like you're running a simulation alongside the real world to try to get a sense of how things will actually play out in the real world.

Why not think that we should be doing something like that? In other words, instead of employing the algorithms just yet, just testing them so that we can actually get to a better efficacy at a certain point. So we can say, look, these things are perfect. They never fail. We've run them for so long that the data are perfect. I'm skeptical that they would stay perfect, but the point is, if we have a greater sense of their ability, I'd be more inclined to use them. I'm also worried that—and you all know this at the level of hearts and minds—when you kill innocent people, innocent guys on tractors, you're likely to find yourself in a situation where you're producing more adversaries and creating a Whack-a-Mole problem that's worse than if you had apprehended the guy and then realized that he's not the right guy. The consequentialist perspective says we know we're causing harm, but in the long run, I think it's a worthwhile point.⁵

STRAWSER: The problem with consequentialism is that it's always relying on prediction. One would have to have a stronger epistemic prediction that it really will work out in the long run for your argument to work. You're saying that you have greater epistemic confidence in increased future adversarial conflict and loss of life due to the technology, than that there is a way for us to achieve our goal *now* without having knowingly failed the evidentiary standard for killing when we think it's justified in the present. You'd have to have a lot of confidence—a tremendous amount of confidence—in that prediction, and that's my issue with the consequentialist move here. Consequentialism is certainly a valid approach to take, but for it to be sound every time, we'd have to have a crystal ball. When we don't

have the required epistemic confidence, I worry we are trading one near-certainty—present moment knowledge that an action is wrong—with less certain predictions that the scales will eventually balance.

DAVIS: I also worry that the calculus that we'd do more good than harm over the long run is something we'd resort to a bit too quickly. But the point is a good one.

SPEAKER 2: I was participating in the Warfare Innovation Workshop last week, and my team was actually debating justified killing. We need to use the kill chain as a framework to understand how we make decisions to kill the targets without algorithms. Basically, once you fix, find, and track your objective, it goes to the operations center and the command has to do many, many activities: they have to check rules of engagement, the law of armed conflict, probably estimate collateral damage, while not even knowing if that target is valuable, or if there are more valuable targets that you are more interested in. So there are many things that are going on that machines as of now are not able to do. If we want the machines to do the killing, they have to actually do this process, these steps in the kill chain process.

As of now, there are two types of artificial intelligence: we have narrow artificial intelligence, which includes things like computer vision, detecting objects, very little tasks, as opposed to artificial general intelligence, which is like machines performing the same things that humans do and even better. Scholars agree that it would take hundreds of years to achieve that kind of performance because you need to model perceptions and emotions, and we're not there yet. So we concluded that if we want to leverage algorithms to make decisions, we needed to change the kill chain process. Everybody was saying, "Yeah, man in the middle, man in the middle." But what if the machines are giving you all the information and you just have to say, "Yes, press the trigger," but they are training on bad information, like the case of the Man in the Purple Hat? Somehow we need to guarantee that the man in the middle does not have to be involved in the decision whether to kill, but is guaranteed to be training the algorithm. He can feed new information into the algorithm so it will train to process information as we humans want it to. We also recommended changing our military planning process, so, in the same way that we have appendices for operational assessment—how to collect information—perhaps we need an appendix for how to incorporate this information to train algorithms, so we don't make the wrong decisions.

Everybody was saying, "Yeah, man in the middle, man in the middle." But what if the machines are giving you all the information but are training on bad information?

DAVIS: Does it strike you as feasible or plausible to make the people who are training algorithms the same people who are making the decisions about when specifically to use them? That seems like a lot on them.

SPEAKER 2: Somehow the process has to involve the guy who trains the algorithm: the operators, the decision makers. If you don't include these people in the process of training the algorithm, you're only relying on black boxes. There's a whole field called machine-learning interpretability—it doesn't only happen in the military—but if you use an algorithm to help you detect diseases in an x-ray, for example, you don't want to rely only on a black box. With machine-learning interpretability, you can definitely see where the algorithm is looking at the image. You can avoid bias for race and gender. Machine learning is already working dependably in many little fields, so people start to trust the algorithms, because right now they're only doing little tasks.

We are talking about fully autonomous systems for defensive purposes. Imagine a hypersonic missile. You cannot rely on calling your boss: "Hey, we should . . ." There isn't time. Perhaps you need your defense system to be fully autonomous, but for offensive operations involving this stealthy assassin role for the machines, then you will need the man in the middle. You also have fully autonomous systems that can do things that help the force. For instance, if there's a big fire and you need to rescue people, you probably don't want to risk people's lives to do it; you want a fully autonomous system. Right now at the United Nations, they are trying to ban legal autonomous weapons systems. The narrative that they are selling is killer robots, not this stealthy assassin role for the machines. So basically, they're going to end up banning all the fully autonomous weapon systems: the ones that really help in the military for good purposes, and also the killing machines.

DAVIS: You've made a lot of great points there. Thank you for your perspective.

SPEAKER 3: I would argue that the epistemic system is going to depend on the theater of war. Are we in a limited conflict? Are we in an unlimited conflict? Are we waging total war? It's also going to reflect the rules of engagement.

To tap into an earlier speaker's point and your response to it, I think that, at some point, if we ran parallel tests, and we started getting information from an autonomous system that would have improved—maybe not perfected, but improved—our decision making, I think we would have a moral imperative to use it. Otherwise, if we're saying, "Well, yeah, it's only at 98 percent; it's not perfect yet, so we're not going to let the ground force commander or the kill chain have access to this information," then we'll just continue to make mistakes. And we already make mistakes. Everybody who conducts killing makes mistakes at some point.

STRAWSER: The comparison's not in a vacuum. It's against humans.

DAVIS: That's a great point, and it comes out with a lot of these technologies. With predictive policing, for example, it's bad. We mess up a lot. Also, it's really good. It's more effective in many cases than just relying on human officers. These systems can digest 80 years of data simultaneously, which is amazing, and they are surely going to do better than humans in a lot of cases. They're going to expose officers or soldiers to less risk. It's going to result in fewer hours of wasted manpower. That's phenomenally valuable. I think you're right that there's a real challenge here. Shouldn't that mean that we have really strong reasons to use the technology unless we have good evidence that it's bad, that it's getting it wrong in that particular instance? It's a good point. It's a good challenge on the other side to say these are really good, really effective systems, and—it would depend on the specifics, as you say—but in many cases, it seems like to *not* use that data would be like not outfitting our soldiers with shields that we know are really effective in preventing harm. That's a valuable point.

SPEAKER 4: Do you think it reduces risk or just transfers risk to somebody else? In this program, we've learned that all models are wrong, but are sometimes useful. So approaching it like that, there's the target engagement authority, or the UAV operator out in Nevada with a team sitting next to him, and the team says, "Well, the model said this" or "The algorithm said this," and "We were wrong" or "We were justified." Yes or no doesn't really matter. The question is, where did that risk go? You had said that benevolent leaders are looking at this and making improvements, but one other term to add to the rules of engagement might be "imminence." Is the decision based on imminent necessity? Yeah, if a bad guy is a bad guy, we want to find him and eliminate him, but to what point? And if all models are wrong and we authorize lethal force, where does that risk end up? And that goes into the rules of engagement of whatever theater we're in and what is an

acceptable level of risk, because there will be times when we're willing to accept 51 percent.

My concern is that, as a practice—not in a specific isolated instance, but as a practice—we are distributing massive amounts of risk onto innocent people.

DAVIS: It's going to depend on what we're trying to kill him *for*. If we think he's about to go into a stadium and blow up the entire stadium full of people, our evidence threshold looks a little bit different. Not only do I agree, but I endorse that point. In terms of distributing risk, my concern is that, as a practice—not in a specific isolated instance, but as a practice—we are distributing massive amounts of risk onto innocent people. I think that practice needs to be justified, because we're killing lots of targets that we *should* be killing, but we're likely also exposing others to risk, and not just risk of death or harm, but other kinds like broader psychological or existential risks. There are concerns in some cases that drone warfare has prevented groups from gathering in places because they're afraid that they're going to look suspicious, and this is hindering democracy. So there are very small-level things that, taken in the aggregate, could be massively problematic. So in answer to your question, my hunch is that it distributes risk in a way that stands in need of a justification. I'm not saying it's unjustified; it depends on the particulars, but I have questions about that.

SPEAKER 5: Building out a point you brought up earlier, you've got to distinguish where the algorithm is functioning. Right now, the sensor is agnostic. The sensors are pulling in data. The human is looking at the data, or the algorithm is sifting through the data, or usually both. That's what we're doing right now. In my opinion, the weight behind your argument has to show that the algorithm is less accurate than the human. Having been there and done this firsthand, I can tell you that humans get impatient. We do a lot of strikes because we haven't done a strike lately, and it's close enough. It's good enough. We're pretty sure that they're all bad anyway. That's what humans are doing right now.

STRAWSER: That's a pretty low bar, and it could be that you think that's wrong, and you could think that they're both wrong.

SPEAKER 5: True, but which is less wrong? In your argument, you're using the term "bad." I don't know that "bad" is an appropriate term to use. Is it better or worse than the

humans who are currently making mistakes? Now we've got some leeway. In some theaters, there's a lot of leeway for making mistakes. Nobody ever finds out. Nobody ever knows. Nobody really cares. But is the algorithm better or worse than the humans? Because the humans are making mistakes. The sensors that are collecting the data are the same sensors for either side.

DAVIS: Suppose we had an algorithm that replaced a jury. It's a jury algorithm. We don't need people anymore, just a jury algorithm, and based on all the things that are said in the rules and whatever, it determines guilt or innocence. We say, look, it only sends innocent people to jail 10 percent of the time. Let's say that human juries do it maybe 15 to 20 percent of the time. I'm just making these numbers up, but let's hypothesize. Would we say, hey, that algorithm is good, and we should start using it? My temptation is to say that both of those are way too high. I'm skeptical about using the 10 percent, and saying, look, the algorithm told us to do it. We're good! Clean hands! No need to worry about it, and in fact, we might be using it more often, taking trials to the jury algorithm more often because we're confident in this system. My concern is that its being slightly better in some instances, or even on average, is not enough. It might be that that's better than the alternative, but I'm not sure that that means we should rely on it, or we should use it. I see the argument in the other direction, too.

STRAWSER: There are probably stories about the Man in the *Green Hat*, where the algorithm got it right and the human operator got it wrong, and the human operator overruled the algorithm, and they're like, oh, damn, we should have listened. It's sort of a math question. Actually, there are really two questions here: what is ethically the right evidentiary standard that needs to be justified, depending on the stakes, depending on all the other contexts, in order to say that we're ethically justified to do this based on this confidence level? That's the main question, and then you're asking, secondarily, could this technology ever meet that threshold? Now, maybe your point is that perhaps the algorithm can or cannot, but humans aren't achieving it in the first place, which is just depressing. But that doesn't answer the question, right? Because they both could fail.

DAVIS: You might say it's the lesser of two evils, or it's the better of bad alternatives, but I don't think that means we should use it. It might just mean slightly better.

ABOUT THE AUTHOR

Dr. Jeremy Davis teaches philosophy at the University of Florida.

This is a work of the US federal government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

NOTES

1. Deputy Secretary of Defense, "Memorandum: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," 26 April 2017: <https://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf>
2. Annie Jacobsen, *First Platoon: A Story of Modern War in the Age of Identity Dominance* (New York: Dutton, 2021).
3. A Ouija board, or spirit board, is a simple device that is said to channel the psychic energy of its users to answer questions.
4. *Minority Report*, directed by Steven Spielberg (2002; Hollywood, CA: Paramount Pictures, 2010), Blu-Ray.
5. The most prominent example of the philosophical view called consequentialism concerns the moral rightness of acts. It holds that "whether an act is morally right depends only on the consequences of that act or of something related to that act, such as the motive behind the act or a general rule requiring acts of the same kind." See "Consequentialism" in the Stanford Encyclopedia of Philosophy, rev. 3 June 2019: <https://plato.stanford.edu/entries/consequentialism/>

Publications

Western Intervention and Informal Politics: Simulated Statebuilding and Failed Reforms

Troels Burchall Henningsen

London: Routledge 2022

USD \$128

210 pages

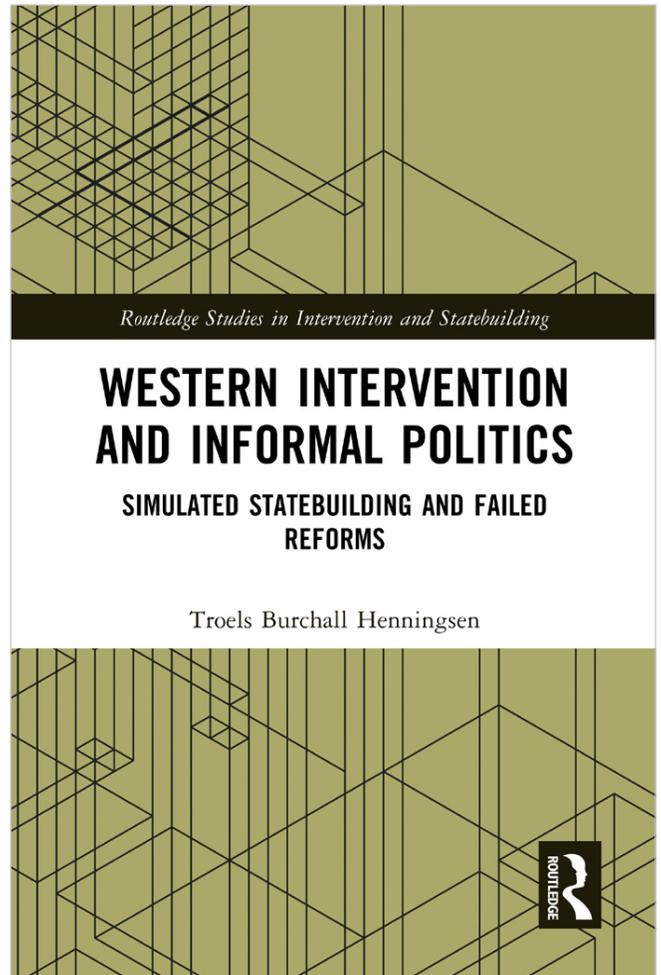
This book examines the political and military dynamic between threatened local regimes and Western powers, and it argues that the power of informal politics forces local regimes to simulate statebuilding.

Reforms enabling local states to take care of their own terrorist and insurgency threats are a blueprint for most Western interventions to provide a way out of protracted internal conflicts. Yet, local regimes most often fail to implement reforms that would have strengthened their hand. This book examines why local regimes derail the reforms demanded by Western powers when they rely on their support to stay in power during existentially threatening violent crises. Based on the political settlement framework, the author analyses how web-like networks of militarized elites require local regimes to use informal politics to stay in power. Four case studies of Western intervention are presented: Iraq (2011-2018), Mali (2011-2020), Chad (2005-2010), and Algeria (1991-2000). These studies demonstrate that informal politics narrows strategic possibilities and forces regimes to rely on coup-proofing military strategies, to continue their alliances with militias and former insurgents, and to simulate statebuilding reforms to solve the dilemma of satisfying militarized elites and Western powers at the same time.

This book will be of much interest to students of statebuilding, international intervention, counter-insurgency, civil wars, and international relations.

About the author

Troels Burchall Henningsen is an assistant professor in the Institute for Strategy and War Studies at the Royal Danish Defence College.



*Baghdad Underground Railroad:
Saving American Allies in Iraq*

Steve Miska

Onward Press, 2021

USD \$16

306 pages

In 2007, Iraq was in the midst of violent sectarian cleansing. Col. Steve Miska led a team within the 2nd Brigade, 1st Infantry Division (known as Dagger Brigade) that established an underground railroad from Baghdad to Amman to the U.S. for dozens of Iraqi interpreters facing near-certain death at the hands of the “death squads” that hunted down and slaughtered interpreters and their families.

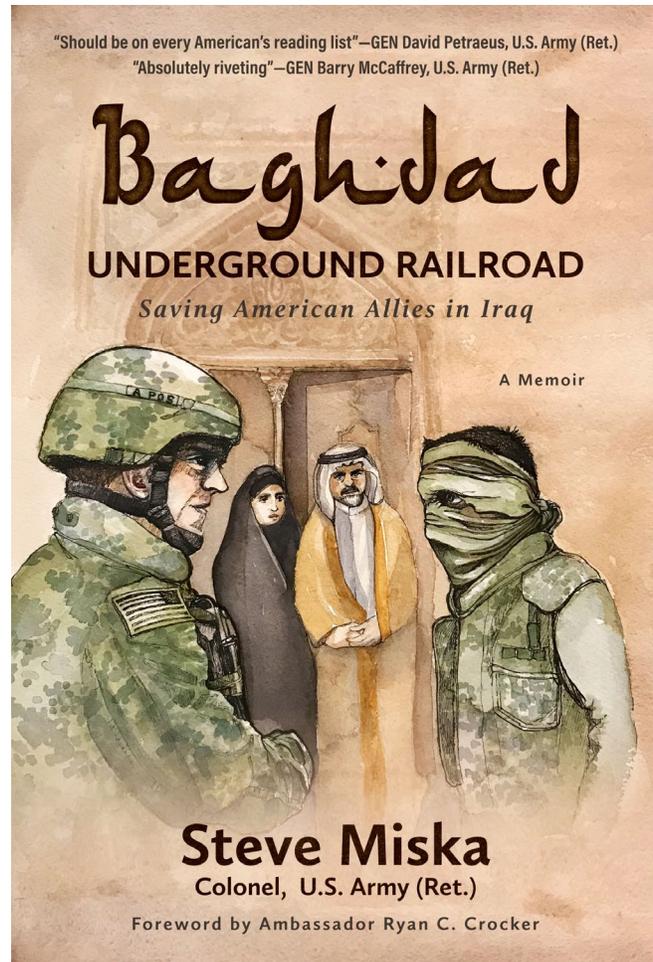
The mostly young men and women who embraced American idealism risked their lives to support U.S. service members in countries where understanding the language, the people, and the contours of the culture are often a matter of life and death. Yet, according to recent estimates, more than 100,000 interpreters and at-risk family members remain in Iraq and 70,000 remain in Afghanistan, each in grave danger.

The plight of Iraqi and Afghan interpreters left behind by the United States remains one of the most significant human rights issues of the Global War on Terrorism, America’s longest, and ongoing, military conflict.

Baghdad Underground Railroad is a sober reminder of the far-reaching human and national security consequences of abandoning U.S. allies in countries of conflict. Above all, it is an exploration of universal questions about hope, brotherhood, and belonging—questions that strike at the heart of who we are as a people and as a nation.

About the author

Col. Steve Miska served as an officer in the United States Army for 25 years before retiring in 2015. From 2011 to 2012, Steve served in the White House as Director for Iraq on the National Security Council. He has written extensively about the need to protect soft networks, and has acted as an advisor to several non-profits that aim to support and protect foreign military interpreters,



including No One Left Behind and the International Refugee Assistance Project. He is the Founder & CEO of Servant Leader Citizen (SLC) Consulting, which exists to educate others about national security and counterterrorism issues in an increasingly global environment, and executive director of the non-profit First Amendment Voice, a nonpartisan effort to reinvigorate civic awareness about First Amendment issues.

Image Credits

Page 1 and 5: Photo by Airman 1st Class Joseph Morales, Joint Base McGuire-Dix-Lakehurst Public Affairs.

Page 8: Senior Master Sgt. Darrick Mischke, the Petroleum, Oils and Lubricants (POL) superintendent assigned to the 119th Logistics Support Squadron, prepares to accept a “Jet-A fuel” delivery at the North Dakota Air National Guard Base, Fargo, North Dakota, 2 May 2018. Photo by Senior Master Sgt. David Lipp.

Page 11: Solar Panels at Bear River Migratory Bird Refuge, Utah. USFWS Mountain-Prairie, Public domain, via Wikimedia Commons.

Page 12: US Air Force photo by Nick Tarasenko, AFRL/RDTA, Official United States Air Force Website, Public domain, via Wikimedia Commons.

Page 16: Mapboard at the NATO Allied Land Command (LANDCOM) Headquarters, 10 April 2019. NATO photo by U.S. Army Lt. Col. David Olson, LANDCOM Public Affairs.

Page 18: Photo by Lance Cpl. Elijah Abernathy.

Page 19: US Marine Corps photo by Lance Cpl. Diana Sims.

Page 26: A US Air Force contractor uses a voltmeter to test the amount of electrical current going through wires at Yokota Air Base, Japan, 15 January 2021. Photo by Jeremy Croft, US Army Corps of Engineers, Sacramento District.

Pages 29 and 30: US Air Force photo by Airman 1st Class Joseph Morales, Joint Base McGuire-Dix-Lakehurst Public Affairs.

Page 34: Armenian soldiers patrol at the checkpoint outside Agdam to let last vehicles leave the region late on 19 November 2020. Photo by Karen Minasyan/AFP via Getty Images.

Page 36: Golden, CC BY-SA 4.0, via Wikimedia Commons

Page 38: Photo by Resul Rehimov/Anadolu Agency via Getty Images.

Page 42: CCDC Army Research Laboratory, Public domain, via Wikimedia Commons.

Page 47: Composite Special Operations Component Command (C-SOCC) with Belgium and Denmark as a NATO Response Force. Ministerie van Defensie, CC0, via Wikimedia Commons.

Page 49: Photo DigitalGlobe via Getty Images/ISIS via Getty Images.

Page 50: Helicopter Weapon Instructors Course 2020. Ministerie van Defensie, CC0, via Wikimedia Commons.

Page 54: Marines with Marine Corps Forces Cyberspace Command observe computer operations 5 February 2020 in the cyber operations center at Lasswell Hall, Fort Meade, Maryland. Original photo by Staff Sgt. Jacob Osborne, US Marines. Photo has been modified.

Page 56: Photo by Staff Sgt. Alexandre Montes, 70th ISR Wing.

Page 60: US Air Force photo by 432nd Wing/432nd Air Expeditionary Wing.

Terms of Copyright

Copyright © 2022. The copyright of all articles published in *CTX* rests with the author(s) of the article, unless otherwise noted. The *Combating Terrorism Exchange (CTX)* is a peer-reviewed, quarterly journal available free of charge to individuals and institutions. Copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research, or educational purposes free of charge and without permission, except if otherwise noted. Any commercial use of *CTX* or the articles published herein is expressly prohibited without the written consent of the copyright holder.

Call for Submissions

The *Combating Terrorism Exchange* (CTX) is a quarterly peer-reviewed journal. We accept submissions of nearly any type, from anyone; however, submission does not guarantee publication. Our aim is to distribute high-quality analyses, opinions, and studies to military officers, government officials, and security and academic professionals in the irregular warfare community. We give priority to non-typical, insightful work and to topics concerning countries with the most pressing terrorism and CT issues.

Submission Guidelines

For detailed submission guidelines, go to <https://GlobalECCO.org> and click on the CTX Home link. Then click on Submissions in the left menu bar.

CTX accepts the following types of submissions. Please observe the following length guidelines:

- **academic analyses** (up to 6,000 words)
- **reports or insightful stories from the field** (up to 5,000 words)
- **photographic essays**
- **video clips** with explanation or narration
- **interviews** with relevant figures (videos no longer than 15 minutes, transcriptions no longer than 6,000 words)
- **book reviews** (up to 2,000 words), review essays (up to 2,000 words), or lists of books of interest (which may include books in other languages)
- reports on any **special projects**
- Any kind of submission can be **multimedia**.

Submissions should be sent in original, workable format. In other words, we must be able to edit your work in the format in which you send it to us, such as Microsoft Word—no PDFs, please.

Submissions must be in English. Because we seek submissions from the global CT community, and especially look forward to work that will stir debate, *we will not reject* submissions outright simply because of poorly written English. However, we may ask you to have your submission edited before submitting again.

Ready to Submit?

By making a submission to CTX, you are acknowledging that your submission adheres to the requirements listed above, and that you agree to the CTX Terms of Copyright, so read them carefully. The CTX Terms of Copyright appear at the end of page 67.

Submit to CTXEditor@GlobalECCO.org

If you have questions about submissions, or anything else, contact CTXEditor@GlobalECCO.org

Submission Requirements

Submissions to CTX must adhere to the following:

- Submissions must be original and not have appeared in any other publication.
- The work must be copyedited for basic errors *prior to* submission.
- Citations should adhere to the *Chicago Manual of Style*. See the latest version at <http://www.chicagomanualofstyle.org/home.html>
- The work submitted may not be plagiarized in part or in whole.
- You must have permission to use any images, videos, or statements included in your work.
- You must agree to our Terms of Copyright, which appear at the bottom of page 62.
- Include a byline as you would like it to appear and a short bio as you would like it to appear (we may use either, or both).

