

CTX

Volume 10, No. 2 2020



ISSN 2162-6421 (online)
Summer 2020



CTX

EDITORIAL STAFF

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

EDITORIAL REVIEW BOARD

VICTOR ASAL
University of Albany, SUNY

CHRIS HARMON
Marine Corps University

TROELS HENNINGSEN
Royal Danish Defence College

PETER MCCABE
Joint Special Operations University

IAN RICE
US Army, (Ret.)

ANNA SIMONS
US Naval Postgraduate School

SHYAMSUNDER 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 Editor

The air is smoky outside my office (a room in my house better known as the kitchen), officially “unhealthy,” but no longer hazardous to breathe. My family and I finally finished emptying all the hastily packed boxes that we took with us when we were ordered to evacuate in the face of a swift-moving wildfire. We were among the lucky ones: our home is safe and life is back to “normal” for now, whatever normal may be these days.

Wildfires throughout the western United States, typhoons in Oceania, economic upheaval and pandemic across the globe; violent extremism is only one of the many catastrophes that are unfolding around us in this strange and unpredictable year. What is predictable is that most of us will continue trying to live our lives the best we can: working from home if we're lucky; venturing out to jobs in now-risky public spaces if we're less lucky; or wondering if we'll ever be lucky enough to find a job again. It is also predictable that certain groups of people will continue to tear at the structures of society in the mistaken belief that building something new is no harder than destroying what exists. Boko Haram, al Shabaab, and the Taliban continue to take innocent lives as indiscriminately as the coronavirus, while al Qaeda and ISIS, it seems, lie low and rebuild. One has to wonder, when a vaccine finally allows us to come out of our houses into the streets and stadiums again, will the extremists be far away? Compassion and generosity can be hard to come by when anger and fear roam free, but they are what can bring us through these painful times.

This issue begins with a look at a special counterterrorism unit in the Netherlands that combines members and tactics of the police and special forces. Based on his work with this unit, the author sees ways in which the Netherlands' SOF might improve its effectiveness by adopting and adapting certain police methods. Next up, Glenn E. Robinson's article on what he terms “movements of rage” introduces a new concept with which to understand highly violent movements across cultural, religious, and national boundaries. It focuses on sociopolitical movements that are characterized by nihilistic violence and apocalyptic ideologies.

The CTX interview brings you former Iraqi Ambassador to the United Nations Feisal al-Istrabadi. Ian Rice and Craig Whiteside spoke with the ambassador

about his experience helping to write a new Iraqi constitution following the overthrow of Saddam Hussein's government, and about his perception of current obstacles to productive relations between Iraq and the United States. Ethicist George Lober then takes an unblinking look at the corrosive effects of dishonesty on human relations, from very personal interactions to institutional hierarchies. Once a lie has been introduced, he posits, it will eat away at trust and corrupt loyalty no matter how much the liar, and even the victim, may imagine otherwise.

We're excited to introduce our new column on serious games, The Game Floor. MSG David Long writes about transforming one of Global ECCO's new games, *CyberWar: 2025*, from a somewhat awkward board game concept into a fast-moving multiplayer online game. He offers insights into how the design and development of an online strategic game tracks with its pedagogical purpose.

Finally, MAJ Daniel Meegan reviews a book by Israeli investigative journalist Ronen Bergman about the covert assassination program carried out by Israel's Mossad over many decades, and MAJ Nate Smith reviews a recent book by Audrey Kurth Cronin on the role that technological innovation is playing in twenty-first-century terrorism.

Be sure to take a look at the latest publications from the Joint Special Operations University.

CTX is written by, for, and about you and your fellow counterterrorism professionals. Our mission is to bring you stories, essays, research, and ideas that will inspire and encourage you as you pursue your mission of combating violent extremism wherever it arises. What would you like to share with the community? What ideas do you have to make *CTX* even better? Write to us at CTXSubmit@GlobalECCO.org and follow Global ECCO on Facebook.

As always, stay safe and stay in touch. We look forward to hearing from you.

Elizabeth Skinner
Editor, CTX

Inside

Letter from the Editor
Elizabeth Skinner



06

What Special Operations Forces Might Learn from the Police: Three Observations
By Major, Royal Netherlands Marine Corps



34

THE GAME FLOOR
Cyberspace Operations Training using *CyberWar: 2025*
By David Tyler Long, US Army



12

Movements of Rage
By Glenn E. Robinson, US Naval Postgraduate School



40

THE WRITTEN WORD
Rise and Kill First: The Secret History of Israel's Targeted Assassinations
By Ronen Bergman
Reviewed by MAJ Daniel Meegan, US Army Special Forces



19

CTX INTERVIEW
Amb. Feisal al-Istrabadi
Interviewed by Craig Whiteside, US Naval War College and COL Ian Rice (Retired), US Army



44

THE WRITTEN WORD
Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists
By Audrey Kurth Cronin
Reviewed by MAJ Nate Smith, US Air Force Special Operations Command



28

ETHICS AND INSIGHTS
On Truth, Lies, and Loyalty: Part One
By George Lober



48

PUBLICATIONS

ABOUT THE CONTRIBUTORS

George Lober retired as a senior lecturer from the Defense Analysis department of the US Naval Postgraduate School (NPS) in 2016. Prior to his retirement, he initiated and taught a course in Critical Thinking and Ethical Decision Making.

Ambassador Feisal Amin Rasoul al-Istrabadi grew up in both the United States and Iraq. He received his JD from the Indiana University (IU) School of Law in 1988, and LLM and SJD degrees from Northwestern University. After returning to Iraq, Istrabadi helped draft Iraq's Transitional Administrative Law and served as legal advisor to the Iraqi Minister for Foreign Affairs. In 2004, al-Istrabadi was appointed Ambassador, Deputy Permanent Representative of Iraq to the UN. He returned to the United States in 2007, where he now serves as an Associate Director of the Center for Constitutional Democracy at IU School of Law, and is the founding director of IU's Center for the Study of the Middle East. In 2015, al-Istrabadi was elected as a member of the American Academy of Arts and Sciences.

US Army Master Sergeant David "Ty" Long is a Senior Enlisted Advisor for the Department of Defense. He earned his MS degree from NPS, where he created and developed the strategic game *CyberWar: 2025*, based on his thesis research. He has published "Wargaming and the Educational Gap: Why *CyberWar: 2025* was Created" in the Spring 2020 issue of *The Cyber Defense Review*. Long is also a senior software engineer and cyber researcher for the US Department of Defense.

Major Daniel Meegan is a US Army Special Forces officer. After commissioning in the infantry, he served at the Joint Multi-National Readiness Center in Germany and in Afghanistan with the Romanian-American Battlegroup. He has deployed multiple times throughout the Middle East, and is currently pursuing a Master's degree in Defense Analysis from NPS. Major Meegan is a recipient of the Department of the Army's General Douglas MacArthur Leadership Award.

Ian Rice is a retired US military officer who has served in a variety of overseas assignments at the tactical, operational, and strategic levels, most notably in Afghanistan, Iraq, and Korea. His most recent assignment in Iraq was with the United States' Diplomatic Mission to Iraq, where he served as director of the Tribal Engagement Coordination Cell during Operation Inherent Resolve.

Dr. Glenn E. Robinson is a professor of Defense Analysis at NPS and is affiliated with the Center for Middle East Studies at the University of California, Berkeley. He joined NPS in 1991, where he specializes in Middle East studies, social movement, US Middle Eastern policy, and political violence and jihad. Dr. Robinson earned his MA (1988) and PhD (1992) in political science from UC Berkeley. He has written several books on the Middle East and the Palestinians; his latest book, *Global Jihad: A Brief History*, is forthcoming in November 2020 from Stanford University Press.

Major Nate M. Smith is a career pilot with the United States Air Force Special Operations Command. He is currently studying Irregular Warfare in the Defense Analysis department at NPS. He is a graduate of the US Air Force Weapons School and has deployed in support of multiple contingency operations in Africa and the Middle East.

Dr. Craig Whiteside is a professor of theater security decision making for the Naval War College Monterey. He earned a PhD in political science from Washington State University, where he also taught American government and national security affairs. His dissertation investigated the political worldview of the Islamic State of Iraq (2003–2013). Dr. Whiteside served as an infantry officer in the US Army and is an Iraq war veteran. He is a graduate of the US Military Academy and the US Army Command and General Staff College.

The author of "What Special Operation Forces Might Learn from the Police: Three Observations" is a major serving in the Royal Netherlands Marine Corps.

COVER PHOTO

A commemorative ceremony held for Qassem Soleimani, commander of Iranian Revolutionary Guards' Quds Forces, who was killed in a US airstrike in Iraq, in Tehran, Iran, on 9 January 2020. (Photo by IRANIAN SUPREME LEADER PRESS OFFICE / HANDOUT/ Anadolu Agency 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 nongovernmental organization or agency of the United States of America or any other country.

TERMS OF COPYRIGHT

Copyright © 2020 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.





What Special Operations Forces Might Learn from the Police: Three Observations

by Major, Royal Netherlands Marine Corps

AT AROUND 11 O’CLOCK IN THE MORNING ON 18 MARCH 2019, a fellow Marine and I were running through the woods near our base in the Netherlands, chatting as we ran. It was warm, beautiful weather and we had a lot to talk about because we had not spoken to each other for some time. Suddenly, my cell phone rang. There was an “alarm” notice on the screen. I listened to the voicemail, which told me that there had been a terrorist attack in Utrecht, the city where I live.¹ I said to my colleague, “They forgot to say, ‘This is an exercise.’” However, it was not an exercise. A terrorist had just shot and killed three people in a tram and wounded several more.

At that time, I was the squadron commander of a SOF domestic counterterrorism unit that operated as part of a joint endeavor between the Dutch National Police and the military. In the Netherlands, this joint unit leads the domestic fight against both high-impact crime and terrorism. It is, as far as I know, a unique kind of national security cooperation, in which police and military personnel operate together on a daily basis under police command, drawing on and integrating institutional qualities from both organizations. Integration can be a challenging process at times, but it has also provided valuable insights for both organizations. Although the operational environment and context of police and SOF work differ in many ways, I believe that any SOF unit that works in counterterrorism may learn something useful from the Dutch experience.

Special forces, as a branch of the military, train and work-up for most of the year and may be deployed abroad for months on high-risk assignments. When they arrive in their area of operations, their local network connections, situational

On 18 March 2019, a member of the Netherlands' special police forces patrols in Utrecht, near a tram where a gunman opened fire, killing at least three persons and wounding several in what officials said was a possible terrorist incident.

The Department of Special Interventions' integration of military and police units goes further than it does elsewhere.

awareness, and time to sort effects tend to be limited. The police, in contrast, train only occasionally, and they operate daily in areas where they often have worked and even lived for years, and where they may belong to extensive professional and social networks. Police operations almost always have lower levels of risk than typical SOF operations. In this respect, the Dutch SOF units learn from their police colleagues what it takes to operate successfully within your own country, in your own city, and sometimes even on your own street. The police, for their part, learn from the SOF how to plan, coordinate, and conduct nationwide counterterrorist operations in which multiple suspects have to be arrested at the same time.

In this essay, I make some observations regarding signature management, interagency collaboration, and hyper-enabled units, and briefly discuss the potential application of each one in SOF operations.

The Dutch Joint Counterterrorism Endeavor

Since 1972, a unit within the Royal Netherlands Marine Corps has had responsibility for domestic counterterrorism. This dedicated CT unit has gone through several restructurings and name changes since its founding; currently, it is one of the operational squadrons of the Netherlands Maritime Special Operations Forces (NLMARSOF). Although it is a military SOF unit under the command of the Dutch Ministry of Defense, during domestic operations the unit works under the command of the police as part of the joint Department of Special

Interventions (DSI), which apprehends suspects in significant police investigations and responds to terror attacks, such as the terror attack in Utrecht. It is somewhat similar to the joint models used in other Western European countries, but the DSI's integration of military and police units goes further than it does elsewhere. For example, the operators of the NLMARSOF squadron wear military uniforms when they are at their base, but they wear police uniforms during operations. Many of the NLMARSOF operators have an unmarked duty car in which they store their weapons and equipment while they are off duty, just as the police officers do. Also, the operators have identification cards for both organizations and are fully integrated with police officers in small teams for everyday operations. In a typical career within NLMARSOF, operators rotate jobs every two to three years on average, which results in a good mix of experience throughout the unit. They are encouraged to spend a rotation with the DSI, and also on the international-focused squadron, the training squadron, and the NLMARSOF staff.

Three Observations from Working in the DSI

My work in the DSI has shown me that certain aspects of the way police operate may have some value for SOF. Three in particular stand out: the importance of being able to rapidly change a unit's signature in a way that adds value to the overall mission; "slowing down" job rotations so that personnel can build relationships in the communities where they are operating; and integrating a team of analysts into the unit so that the real-time "hyper" number of

Police forces and emergency services investigate a shooting at the 24 Oktoberplein in Utrecht on 18 March 2019.



data streams coming in during an operation are converted into one operational and actionable picture.

Signature Management

To do their work of maintaining public order and enforcing laws, the police, on the one hand, have to be visible on the streets. On the other hand, they must not be visible during operations such as surveillance and infiltration, so signature management is an essential aspect of police work. Even so, in my experience, the DSI assumes that both its SOF and regular police operators will become visible at some point; operators know that they can be filmed and live-streamed on television at any moment.² In some instances, videos show the actual procedures of the teams in near-real time on TV or social media.³ The video footage is often rebroadcast over and over again in compilations by news agencies.⁴ In the Utrecht terrorist case, the mayor of the city directed all citizens to stay inside buildings.⁵ The streets were empty, which meant that the unmarked vehicles of the DSI could easily be spotted by the news agencies and live-streamed on Dutch and international television.⁶

DSI operators are very aware that they must be able to explain and justify every step they take during their work.

As a result, DSI operators are very aware that they must be able to explain and justify every step they take during their work. As an organization, the DSI proactively prepares media statements and monitors social media to respond instantly to physical or digital visibility, and tries to connect a particular action or operation to a higher purpose.⁷ This could be the overarching purpose of a safe and secure country in the case of terrorism, for instance, or one more directly tangible to viewers, such as the safety of their city or province. For example, if a drug network that caused a lot of local violence is taken down, the official statement regarding that operation might directly refer to the violence and the goal of restoring safe streets.

The purpose of the Utrecht operation was clear to the public. However, associated activities that were taking place simultaneously in other parts of the country, such as tracking down leads to potential accomplices, were not intended to be visible. During these activities, the DSI units applied stealth tactics, blending into the local pattern of

Netherlands Maritime Special Operations Forces



life so as not to attract attention and possibly alert potential suspects.

SOF units might learn something from the police about how to rapidly change the unit's signature within one operation. During domestic operations, SOF units experience considerable freedom of movement and few, if any, cultural differences within their operating environment. I do not advocate that Western SOF units on a strike mission try to blend into the local population of Afghanistan or Iraq, for example. That would, obviously, be impossible. However, the world is shifting toward a form of Great Power competition that seems likely to bring an increase in clandestine SOF operations in the grey zone. In some of these environments, SOF units might be better off if they are able to constantly and consciously assess their signature and adjust to the situations they encounter. As a result, they might need to operate like the DSI: visibly in one area but covertly in another.

Interagency Collaboration

Police need to collaborate with numerous other governmental organizations daily in the course of their work. In the Netherlands, I have noticed that those collaborations are often based on long-lasting relationships and personal trust. As noted earlier, members of the police have a geographical advantage because of the fact that they typically live and work in the same area. Therefore, it is easier for officers to build long-lasting relationships with officials that enhance interagency cooperation. Furthermore, both the police and these other organizations have relatively few staff changes, which means that members are able to form durable ties both among individuals and between their agencies. Both sides seem to rely heavily on these established social networks to do their jobs. At the time of the terrorist attack, members of the Utrecht police, justice department, and city government knew each other well and had often worked together in previous emergencies or crises. In fact, it is typical for leaders of the respective agencies throughout the Netherlands to hold joint press conferences to emphasize their shared leadership.⁸ The bonds and trust that Utrecht officials had formed earlier helped enormously when they needed to share information and collaborate after the shooting on the tram.

The military's rotation system often prevents the development of personal relationships that make interagency work effective.

In contrast to the close relationships between the police and other government agencies, the military's assignment rotation system often prevents the development of the necessary personal relationships that make interagency work effective. SOF personnel, as in many military units, rotate jobs every two to three years as a means to enhance individual growth and leadership. As an institution, SOF seem to rely heavily on the "organizational machine" that produces leaders rather than on a strategy of building long-term relationships. I do not suggest that SOF should step away from the focus on individual growth and leadership and adopt the local police model, but a golden mean might lie between the two cultures. Slowing down the speed of SOF rotations might not only enable personal growth but also promote valuable intra- and inter-organizational relationships, and thus facilitate interagency cooperation.

Hyper-Enabled Units

The police have an existing and dense network of enablers, such as traffic cameras, investigation teams, and citizen contact. In military terminology, this kind of network is "hyper-enabling." At first glance, the initial development of such an information system might seem to be the primary challenge to creating hyper-enabled responses. In my experience, however, the real problem for the police lies in assessing all the data that comes in from such a network. In the Utrecht case, I arrived at the main police command post about 45 minutes after receiving the alert on my phone and saw that the police still had no clear picture of what had happened and what was happening. The staff were overwhelmed by phone calls, social media postings, and information coming in from officers on the street, but I also noted that the police analysts were closely focused on validating the often contradictory data. To do so, they took a step back and asked more questions, such as: "What was the very first call? What does the log of that call say? Who labeled this as terrorism and why? What other information are we sure is true?" Over the course of that day, I experienced how an operational picture was built based on the information from all those enablers and by additional methods such as, for example, sending units to visit citizens who claimed to have witnessed other shootings in order to assess that information firsthand. The effect of being hyper-enabled is having access to, and the support of, massive amounts of real-time data. Although this leads to a lot of information "noise," it also provides an invaluable opportunity to cross-validate the information, reject what can't be verified, and, subsequently, act on that validated information. In Utrecht, it soon became clear that the terrorist had escaped, and so we began a manhunt.



Currently, the US Special Operations Command is taking the first steps towards creating a hyper-enabled SOF operator.⁹ These initiatives seem to focus on bringing data from an array of enablers to the operator, the idea being that a hyper-enabled operator can outthink his opponent.¹⁰ Based on my experiences, I suggest that SOF commands build on their military institutional expertise of creating and implementing structures so that, in addition to increasing the number of enablers and the amount of data coming in, they establish an analysis system that cross-validates and assesses data before it gets to a unit, let alone to the individual operator.

Larger countries may also benefit from the Dutch experience.

Take, for example, the anecdotal case of a hostage situation on a ship that is anchored near the Somali coast. In this situation, a SOF unit is on standby to respond instantly and release the hostages. This SOF unit has only a few enablers, including a cell of negotiators, snipers with a clear view of the ship, communications interception, and a drone overhead to relay video. In the current era, these are a common set of enablers that generate essential real-time data. Generally, these data streams are directly shared with the SOF unit through its commander. This raw data, however, often produces contradictory information that has to be assessed by the SOF unit. For instance, the negotiators may feel that the Somali spokesman is calmly cooperating, whereas the snipers report people making aggressive movements in the

cabin with the hostages. Furthermore, the communications interception reports telephone calls in which screaming people can be heard in the background.

These are only a few examples of enablers that produce contradictory information. As a rule, the more enabled a unit is, the more data streams exist and the more conflicting information a SOF unit receives. Hence, merely adding sensors and striving to hyper-enable operators would not necessarily help the SOF unit in the hostage scenario to clarify the situation on the ship, but might rather overload the unit with possibly contradictory information and lead to a wrong decision. An obvious solution would be to have all these data streams interpreted by analysts and merged into a tactical assessment that is only then transparently shared with the SOF unit. However, in my experience, the current analytical capacity seems to be geared more toward longer-term strategic reports that are well-thought through but take considerable time to develop. What a SOF unit needs in a hostage situation such as the one described above are analysts who can interpret and integrate real-time data streams in rapidly developing and ambiguous situations. So, instead of focusing effort on hyper-enabling individual operators, I suggest that the first step is to hyper-enable SOF units by training an element of analysts to assess and cross-validate data from a “hyper” number of enablers while working in active, rapidly developing, ambiguous crisis situations.

Conclusion

The Dutch have a working concept for domestic counter-terrorism in which SOF and police are integrated in the

Department of Special Interventions and operate jointly under police command. These combined SOF and police units operate daily on the streets of the Netherlands's cities. While the integration process has not been without challenges, both organizations contribute to the success of the joint venture with their unique institutional qualities. At first glance, the integration of SOF and police may seem to be a realistic option only for smaller nation-states. Although smaller states tend to have smaller institutions, the differences between the institutional aspects of SOF and police organizations, such as their human resources and benefits systems, appear to be of similar scale whatever the size of the country. Thus, larger countries may also benefit from the Dutch experience.

The terrorist attack in Utrecht was a crisis that not only received national and global media coverage but also showed the value of the joint concept, as its operators responded rapidly, effectively, and decisively. How does this story end? Due to the DSI's experience with signature management, its long-term relationships with other agencies and local governments, and its ability to manage hyper-enabled data streams, it was able to resolve the terrorist crisis the same day that I received the alarm on my cell phone. Thanks to surveillance cameras on the tram, we learned the identity of the attacker in about two hours. When we arrested him three hours after that, we could positively identify him through the facial images taken from that video.¹¹ He was tried in court and received a life sentence.¹²

ABOUT THE AUTHOR

The author serves in the Royal Netherlands Marine Corps.

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. Lianne Kolirin and Schams Elwazer, "Utrecht Shooting: Note Found in Getaway Car Suggests Terror Motive," CNN, 19 March 2019: <https://www.cnn.com/2019/03/19/europe/utrecht-attack-letter-intl/index.html>
2. "Eerste Beelden van Aanhouding Gökmen T., verdachten schietpartij Utrecht" [First Footage of Arrest of Gokmen, T. suspect in Utrecht shooting], RTL Nieuws, 18 March 2019: <https://www.rtlnieuws.nl/nieuws/laatste-videos-nieuws/video/4646956/eerste-beelden-van-aanhouding-gokmen-t-verdachte>

3. NOS, "ARNHEM: 7 mannen aangehouden bij antiterreuractie" [ARNHEM: 7 men arrested during counterterrorist operation], YouTube Video, 0:47, 27 September 2018: <https://www.youtube.com/watch?v=7Ph4lhgBgVk>; RTL Nieuws, "Agenten overmeesteren man met getrokken wapen na steekpartij Den Haag" [Police officers with weapons ready arrest a suspect after stabbing incident], YouTube Video, 1:01, 6 May 2018: https://www.youtube.com/watch?v=k06qY19_UVk
4. NOS op 3, "Dit gebeurt erachter de Schermen Tijdens een Aanslag" [This Happens Behind the Curtains During an Attack], YouTube Video, 3:38, 23 March 2019: <https://www.youtube.com/watch?v=K1DQ1pxpH8>
5. Nu.nl, "De gebeurtenissen in Utrecht moment tot moment" [The events in Utrecht from moment to moment], 19 March 2019: <https://www.nu.nl/schietpartij-utrecht/5798385/de-gebeurtenissen-in-utrecht-van-moment-tot-moment.html>
6. Bart H. Meijer, "Dutch police arrest Turkish man suspected of killing three in tram shooting," *Reuters*, 18 March 2019: <https://www.reuters.com/article/us-netherlands-shooting/dutch-police-arrest-turkish-man-suspected-of-killing-three-in-tram-shooting-idUSKCN1QZ10X>
7. "Verdachten in Raadkamer" [Suspect in Court], *Politie*, <https://www.politie.nl/gezocht-en-vermist/dossiers/2019/03-incident-utrecht/dossier-incident-utrecht.html>
8. NOS "Live: Persconferentie gemeente Utrecht" [Live: Press Conference of the City of Utrecht], YouTube Video, 27:59, 18 March 2019: https://www.youtube.com/watch?v=5fLGc_1wIX4
9. Jared Keller, "Inside Special Operations Command's effort to build a 'hyper-enabled operator' who can outthink the enemy," *Business Insider*, 20 December 2019: <https://www.businessinsider.com/socom-effort-to-build-hyper-enabled-operator-to-outthink-enemy-2019-12>
10. Alex MacCalman, Jeff Grubb, Joe Register, and Mike McGuire, "The Hyper-Enabled Operator," *Small Wars Journal*, 6 June 2019: <https://smallwarsjournal.com/jrnl/art/hyper-enabled-operator>
11. "The events in Utrecht from moment to moment."
12. "Dutch Court Convicts Man in Deadly Tram Terrorist Attack," *New York Times*, 20 March 2020: <https://www.nytimes.com/2020/03/20/world/europe/dutch-tram-terrorist-attack.html>

Movements of Rage

by Dr. Glenn E. Robinson, US Naval Postgraduate School



Skulls of those killed by the Khmer Rouge at Cambodia's Choeung Ek Memorial

The purpose of this essay is to introduce special operators to the concept of “movements of rage,” a distinctive form of violent sociopolitical movement that does not fit well into the common categories of terrorism, fourth wave religious terrorism, new terrorism, cosmic war, or other existing definitions of forms of political violence. Movements of rage are typically small and inchoate movements that rarely come to power, but that incorporate justifications of profound violence and apocalyptic ideologies that can be religious or secular. The concept of movements of rage was first described by UC Berkeley scholar Ken Jowitt.¹ I refine and expand the concept in my new book, *Global Jihad: A Brief History*.²

By looking at examples of movements of rage, we can begin to see why they are not easily pigeonholed into existing categories and definitions. Movements of rage have emerged out of Maoist, Fascist, Islamist, and other ideological traditions. Perhaps the most well-known example were the Khmer Rouge, who ruled Cambodia from 1975 to 1979 and presided over a genocide of up to two million souls. This Maoist offshoot glorified an imagined Khmer history based on a model of simple peasantry. Who were the enemies who deserved brutal re-education at the least and, in many cases, summary execution? The educated. Cambodians who spoke a European language, who wore European clothing, or even who wore eyeglasses, which denoted the ability to read, were targeted for execution or exile to labor in the countryside. These educated elites were seen by Khmer Rouge leaders as a cultural “fifth column” who brought cultural contamination of the pure Khmer agrarian life into Cambodia.³ Indeed, one of the first actions of the Khmer Rouge when they seized power was to empty the capital city, Phnom Penh, of its inhabitants, because this was the place where such contaminating elites lived. Virtually

Virtually overnight, Phnom Penh became a ghost town, as many of its residents were marched to the killing fields.

overnight, Phnom Penh became a ghost town, as many of its residents were marched to the killing fields outside of town, never to be seen again. This purposeful destruction of the country's "best and brightest," represented what I have called a *gnosicide*—the killing or violent marginalization of the educated stratum, of those with knowledge.

This form of state terror does not emerge naturally from Maoist thought and does not fit into any of the usual categories of violence noted above. The Khmer practiced violence that was nihilistic: not meaningless, but what could be called "root-and-branch" violence, out of all proportion to any legitimate strategic goals. Their ideology was apocalyptic, based on the belief that a sort of non-religious End Times was upon them and that the violent elimination of the sources of cultural contamination was essential to make way for their agrarian utopia. Their leadership—many, ironically, educated in France—did not come from the traditional historic leadership stratum of Cambodia, but rather from more marginal groups and families, particularly provincial elites. Very few studies of political violence try to make sense of this extraordinary episode; most, instead, classify it as an example of state-directed genocide. While that is a true depiction, it does not go far enough in putting the Khmer Rouge into a broader comparative perspective.

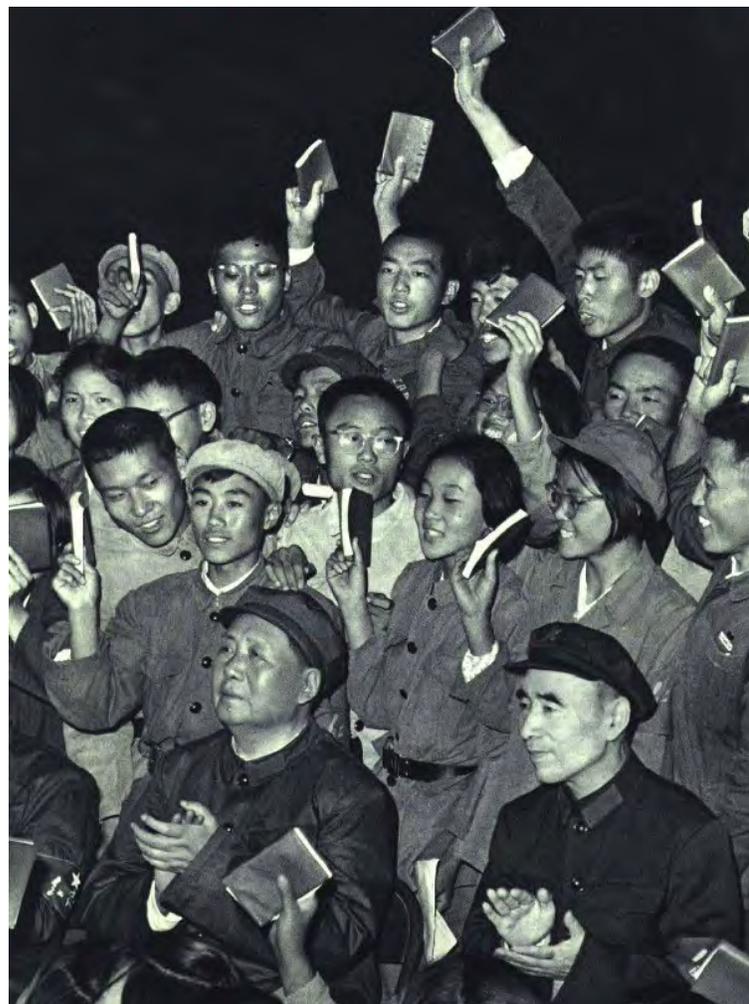
The Khmer Rouge did not have far to look to find an exemplar of a Maoist offshoot that undertook a remarkably similar gnosicide consisting of a murderous attack on a culturally polluting educated stratum: the Red Guards of China. The Red Guards emerged autonomously in 1966 in the chaos of the Cultural Revolution, Mao's attempt to regain the authority that he had lost through his disastrous "Great Leap Forward" program, which had killed millions of citizens and seriously damaged China's economic progress. The young Red Guards saw an opportunity to operationalize Mao's criticism of "bourgeois tendencies" inflicted on China by capitalist infiltrators and corrupters. They set out to attack and murder Chinese intellectuals—those with knowledge. At the height of the Red Guards' reign of terror, from 1966 to 1968, thousands of intellectuals, including schoolteachers and scholars, were killed or beaten. Mao, seeing the power and devotion in these young protégés, promoted their vision and their leaders. Indeed, beyond accepting the wanton murder and destruction of cultural institutions by the Red Guards, Mao implemented two policies of gnosicide that came out of the Red Guards' ideology: the closure of all schools and universities from 1966 to 1972 (and some even longer), and the agrarian "re-education" of high school and university graduates from Beijing in the "Down to the Countryside" campaign, which resulted in hundreds of thousands more deaths. While exact figures are hard to come by, about

as many people died in the Red Guards' orgy of violence as did a decade later in Cambodia.

The very name Boko Haram translates to "education is forbidden."

But examples of movements of rage are found beyond the Maoist world. Some extremist Islamist and jihadi groups have also practiced similar gnosicide. For example, in its origins, the Nigerian group Boko Haram was a prototypical movement of rage. Its very name translates to "education is forbidden"—the education system inherited from British colonial days being viewed as a source of cultural contamination.⁴ Boko Haram's violence has mostly targeted schools and the students being educated in them. Most notoriously, in April 2014, Boko Haram kidnapped 276 schoolgirls from a school in Chibok, Nigeria. Some were executed; a few were released; but most were involuntarily "married" to Boko Haram fighters and were not heard from again. Boko Haram's leaders later pledged loyalty to ISIS. The Taliban, who held power in Afghanistan from 1996 to 2001, are another example of a movement of rage; they viewed Kabul as the capital of cultural corruption and tried to ban all Western

Red Guards with Mao



influences. Anything that was seen as foreign knowledge was removed from the classroom, and all education was prohibited to females. Music was banned and beards were made mandatory for men. The Taliban's austere totalitarianism, rooted in rural and provincial mores and resentments, was not dissimilar to the agrarian nirvana envisioned by the Khmer Rouge.

The most famous examples of global jihad groups, such as al Qaeda and ISIS, are also manifestations of an Islamist version of movements of rage. In both cases, their violence was nihilistic and their ideologies apocalyptic. Al Qaeda is most infamous for its 11 September 2001 terror attacks on the United States that killed nearly 3,000 innocent civilians. But even before then, in a 1998 statement, Osama bin Laden and other al Qaeda leaders had called for the murder of all Americans and Jews, civilian or military, anywhere in the world. This brazen demand for the execution of 350 million souls is the very definition of nihilistic root-and-branch violence. ISIS categorized not only non-Muslim "infidels" (*kuffar*) and "rejectionist" (*rafidun*) Shia as collectively warranting death, but also, essentially, even pious Sunni Muslims who did not agree with the ISIS program. The gore and ghoulishness with which ISIS undertook the execution of its enemies were filmed and uploaded online for the world to witness. The apocalyptic nature of ISIS's ideology was very evident, as Will McCants captured in his aptly named book, *The ISIS Apocalypse*.⁵ Attacks on education were also common in the ISIS "Caliphate," where girls were typically not allowed any education and jihadi ideology replaced actual knowledge in what passed for a curriculum in ISIS schools.

Like Maoism, Fascism has a tendency to spawn or attract movements of rage.

Alt-right members preparing to enter Emancipation Park holding Nazi, Confederate, and Gadsden Don't Tread on Me flags at the 'Unite the Right' Rally, Charlottesville, Virginia, USA.



Fascism, like Maoism, is not in and of itself a movement of rage, but, again like Maoism, Fascism has a tendency to spawn or attract movements of rage. Germany's Brownshirts, an important early component of the Nazi movement, were the best-known example of a movement of rage attached to a Fascist movement. The Brownshirts (or *Sturmabteilung*, literally Storm Detachment), were semi-literate, lower middle class workers from mostly rural origins who acted as a militia of thugs and protectors of the Nazis in the 1920s and 1930s. Once the Nazis were firmly in power and no longer needed the poorly organized and trained Brownshirts, Hitler ordered them purged from the coalition in 1934, during an event known as the Night of the Long Knives. The Brownshirts, like others in the Nazi coalition, fully embraced the doctrine of cultural contamination by impure groups—Jews, Gypsies, gays, the disabled—and sought not just the ritual removal of these groups from the pure Aryan nation, but their actual physical destruction. Education was one indicator of such cultural contamination, so book burning was a common occurrence under Nazi rule.

Not all White Nationalists constitute a movement of rage, but many do. Like the Brownshirts before them, many White Nationalists do not have college degrees, come from rural areas, and blame "coastal" and other elites for the cultural contamination of an imagined once-pure society. In Europe and the United States, White Nationalists find such cultural contamination primarily in the form of non-white immigration. They also find cultural contamination in fifth-column elements who threaten the purity of white society; this was the meaning of the infamous chant at the 2017 White Nationalist Unite the Right Rally in Charlottesville, Virginia, that "Jews will not replace us." While gnosicide in some form has not occurred to date in the United States, it is significant that, of Republican Party members and independents who lean Republican, nearly twice as many view colleges and universities negatively as view them positively—a trend that is rapidly spreading.⁶ White Nationalist acts of mass violence have been directed against the impure immigrant populations (e.g., attacks in Christchurch, New Zealand, and El Paso, Texas), impure fifth columnists (e.g., attacks on Jews in synagogues in Pittsburgh, Pennsylvania, and Poway, California), and the liberal elites who make it all possible (e.g., the 2011 attack on a liberal political summer camp in Norway that killed 77 people, mostly children).

Having established the similarity of some very violent political movements across different cultural and political settings, let us move to precisely defining movements of rage, and to establish why they constitute a unique form of violent political movement. A movement of rage is a distinctive

violent sociopolitical movement that is characterized by three elements:

- nihilistic violence;
- apocalyptic, anti-Enlightenment ideology;
- charismatic leadership.

Let me address each of these characteristics in turn. The word “nihilism” is critical to understanding movements of rage, but can be confusing because it has two different meanings. Nihilism has a philosophical meaning based on the Latin word *nihil*, or “nothing,” and refers primarily to a nineteenth and twentieth century movement of Existentialism founded by Danish theologian and philosopher Soren Kierkegaard (1813–1855). Existentialism holds that there is no intrinsic meaning in life, so that life is literally meaningless. This challenged both religious interpretations of life as having a broader meaning through God, and philosophical interpretations that likewise posited some grander meaning to life beyond biological existence. Existentialism spawned movements in the worlds of art, philosophy, and literature, and its advocates include famous names such as Friedrich Nietzsche, Martin Heidegger, Fyodor Dostoyevsky, Jean-Paul Sartre, and Albert Camus. Those thinking in Existential terms would believe that nihilistic violence is “meaningless violence.” But this is not so. However abhorrent, no politically motivated act of violence is meaningless; there is always a point to it. Those acts of violence that really are meaningless are not political. For example, Stephen Paddock’s sniper attack on a country music festival in Las Vegas, Nevada, in 2017, which left 60 people dead and hundreds injured, appears to have been a meaningless act of violence. Paddock was not part of any political group that we know of, and left behind neither a video nor a written statement of why he was about to murder many strangers. It appears that he set out to murder people simply for his own entertainment, and not for some cause (however deranged). So the Las Vegas shooting appears to have been meaningless violence in the philosophical (Existential) sense of the word. This form of mass murder is very rare indeed.

However abhorrent, no politically motivated act of violence is meaningless.

Far more common is mass murder undertaken under the second, political meaning of nihilism; that is, extreme violence done to destroy a whole society, a system, root and branch. This use of the word nihilism was also a nineteenth century invention, in this case to refer to the writings of the Russian anarchist Mikhail Bakunin. Bakunin and his fellow anarchists wanted to bring down the whole corrupt system



St. Peter's Square, Rome

in Moscow through *extreme* violence; they did not advocate utilizing violence with some sense of surgical precision for a specific goal. So nihilistic violence in the political sense came to mean extreme violence, not meaningless violence. All of the violence noted in my examples above is evidence of either actual extreme violence, such as that undertaken by the Khmer Rouge, or ideological justifications for extreme violence, such as that of al Qaeda. But in none of these cases has the violence been meaningless. Its perpetrators have always had political goals they sought to achieve: some nirvana they believed they were willing into existence.

As Marxism evolved into Leninism and then Maoism in places, it promised material advancement, equality, and greater social justice.

If nihilistic violence is the first characteristic of a movement of rage, then an apocalyptic, anti-Enlightenment ideology is a second characteristic, and that ideology will always have cultural contamination as a feature. The ideology of a movement of rage is distinct from virtually all violent sociopolitical movements over the past century. The vast majority of all violent movements in the modern era have depended on an Enlightenment ideology, be it Communism on the Left, national liberation from the Center, or Fascism on the Right. Karl Marx and the Communists he inspired believed in the scientific march of history: that history was not a series of random events (as Existentialists would argue), but rather, that it unfolded in a systematic, scientific, and predictable fashion. Most importantly, this historical march led at each step of the way to a better society. While Joseph Schumpeter coined the phrase “creative destruction,” it was Karl Marx who argued that capitalism—and its associated creative destruction—was a remarkably vibrant economic system that was superior to the feudal system it replaced. As Marxism



Hitler salutes Brownshirts

evolved into Leninism and then Maoism in places, it took power in many countries and promised material advancement, equality, and greater social justice: in other words, the forward march of history.

The national liberation movements of the twentieth century were also based on Enlightenment ideals, with the promise that their victories would bring liberty and freedom to colonized and oppressed peoples throughout Africa and Asia. Shedding European domination was also a step in the forward march of history. These national liberation movements were an obvious extension of the Enlightenment ideals embodied in the earlier revolutions in France, Britain, and America.

Even Fascism was based on the Enlightenment ideal of material progress, or, in Mussolini's famous phrasing, "to make the trains run on time." The huge monuments and wide boulevards built and planned to be built in Italy and Germany under Fascist rule were testimony to the greatness of their peoples and the advance of civilization under their rule. Even the Vatican was not spared the symbolic greatness of Italian Fascism when Mussolini personally allowed the destruction of the intimate Spina neighborhood to create a giant boulevard leading up to Saint Peter's Square.

Movements of rage are backward-looking, usually to some imagined golden era when life and society were at their best.

Movements of rage do not turn to the Enlightenment for their inspiration. They are instead backward-looking, usually to some imagined golden era when life and society were at their best. Although they were Maoists, Khmer Rouge leader Pol Pot and the Khmer leadership looked to the early Khmer empire (late ninth century to early fifteenth century) as their golden era to emulate. ISIS, Boko Haram, and other jihadi

movements of rage look to the time of Muhammad and his first four successors as that imagined perfect period in history they seek to recreate. White Nationalists in the United States often look to the imagined 1950s as their lodestar, when blacks, women, Latinos, gays, and other cultural contaminants of white patriarchal society were mostly hidden from view.

While movements of rage look back, not forward, to the apex of history, their ideologies also feature a strong element of cultural contamination, which goes a long way toward explaining why those "best days" are always behind them. Cultural contamination tends to include two qualities: the physical manifestations of cultural corruption and the fifth columnists who make it possible. For both the Khmer Rouge and extreme jihadis, it is the West that is the source of cultural contamination. It was the West that ruined pure Khmer society and the West that corrupted Islam and the Muslim world. Thus, attacks against the West are justified and encouraged in order to stop the scourge of further contamination. For White Nationalists today, it is the non-white immigrant population that bears the brunt of the cultural contamination accusations. At the same time, fifth columnists—educated elites—within pure society are also targeted as being vectors for contamination. This is why the Khmer and the Red Guard targeted and often murdered anyone who had the mark of advanced education; this is why most of the people ISIS killed were not Westerners, but rather those Muslims who were considered the bearers of contamination; this is why White Nationalists constantly verbally, and sometimes physically, attack the liberal elites who support policies of cultural contamination. This is why, when they come to power, movements of rage commit gnosicide, terrorizing those with knowledge because, through their knowledge, these elites corrupt the pure, idealized society.

Finally, and not surprisingly, movements of rage tend to have charismatic leadership. The charismatic leader—almost always a man—is awe-inspiring, endowed by his followers with the attributes of a god (the word charisma is originally religious in meaning). Charismatic leaders ask their followers to do hard things in the name of their cause, and often have an aura of prophecy about them. Both Mao and Iran's Ayatollah Khomeini led social revolutions and succeeded against long odds, and both asked their followers to risk their lives for the cause. Even though Mao was a secular charismatic leader, he was often thought to hold a "Mandate of Heaven" (*tian ming*). Khomeini was often whispered to be the returning twelfth imam who had been in occultation for over a millennium (*al-imam al-gha'ib*). Neither of these revolutions was a movement of rage, but both point to the centrality of hard, demanding, charismatic leadership for



Ruhollah Khomeini and people.

any such movement to actually come to power. But what sets the charismatic leadership found in movements of rage apart from that found in other types of sociopolitical movements is the *marginal or provincial* origins of the leaders. These are men (and it is always men in movements of rage) who are not familiar in the halls of power, do not come from elite families, did not grow up in the capital city, and did not go to the best private schools money could buy. Typically, they hail from the provinces, are smart and did well in school, but were never allowed entry into the intimate circles of national power and wealth. They may even be provincial governors or mayors, and often come from families that are locally prominent but not at the national level. Their rage is frequently personal, emanating from what they perceive as their unjust exclusion from national elite status.

Movements of rage are typically weak and almost never come to power. Their resort to excessive violence and their inchoate, backward-looking ideologies do not appeal to very many people. Their leaders can be arrested or killed, which often devastates a nascent movement of rage. States' ability to detect and deal with dissent has only grown stronger in the information age, making it even more unlikely now that a movement of rage will gain enough traction to move forward. That said, movements of rage are deadly. They aspire to kill a lot of people, particularly through communal cleansing of social contaminants. Where governments have ignored the growing threat of a movement of rage, as seems to be the case in the United States with regard to White Nationalism, they have invited much greater levels of violence and terror down the road.

Where governments have ignored the growing threat of a movement of rage, they have invited much greater levels of violence and terror down the road.

Special operators (and others) would do well to add the category of movements of rage to the types of deadly actors with whom they deal, and to distinguish movements of rage from other forms of violent groups that espouse terror. Understanding the distinctions between different forms of violent actors can make all the difference in the world when deciding how best to deal with those groups, and will increase the chances of success in doing so.

ABOUT THE AUTHOR

Dr. Glenn Robinson is a professor of Defense Analysis 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. Jowitt discusses movements of rage (briefly) in two places. See Ken Jowitt, *New World Disorder: The Leninist Extinction* (Berkeley, CA: University of California Press, 1992); and Kenneth Jowitt, *Notes on National Weakness* (Washington, DC: National Council for Soviet and East European Research, 1995).
2. Glenn E. Robinson, *Global Jihad: A Brief History* (Palo Alto, CA: Stanford University Press, 2020).
3. The term "fifth column" refers to a clandestine or subversive faction that seeks to undermine a nation's social and political cohesion.
4. For more on the history of Boko Haram and its ideology, see Muhammad Feyaz, "Understanding the Intensity of Boko Haram's Terrorism," *CTX* 5, no. 1 (February 2015): <https://nps.edu/web/ecco/ctx-vol-5-no-1-february-2015>
5. William McCants, *The ISIS Apocalypse: The History, Strategy and Doomsday Vision of the Islamic State* (New York: St. Martin's Press, 2015).
6. Kim Parker, "The Growing Partisan Divide in Views of Higher Education," Pew Research Center, 19 August 2019: <https://www.pewsocialtrends.org/essay/the-growing-partisan-divide-in-views-of-higher-education/>



Funeral procession of Qassem Soleimani, Tehran

The CTX Interview

Ambassador Feisal al-Istrabadi, Former Iraqi Ambassador to the United Nations

*Interviewed by Dr. Craig Whiteside,
US Naval War College
and COL Ian Rice (Retired), US Army*

ON 31 JANUARY 2020, THE NATIONAL Security Affairs department of the US Naval Postgraduate School (NPS) in Monterey, California, hosted Ambassador Feisal al-Istrabadi for a guest lecture with students and faculty. Afterward, he sat for an interview with Dr. Craig Whiteside and Colonel Ian Rice (Retired) to discuss the rise and fall of ISIS in Iraq and prospects for the future of the US-Iraqi relationship.¹ Istrabadi is a former Iraqi ambassador to the United Nations (2004–2007) and is currently on the faculty of the University of Indiana’s Center for the Study of the Middle East.

CRAIG WHITESIDE: You mentioned in an earlier lecture that you come from a family with a long background in Iraqi politics.

FEISAL AL-ISTRABADI: Yes. Although my parents were not political, the larger families on both sides were politically involved. My family goes back to the foundations of the modern state of Iraq. My paternal grandfather was a member of the Iraqi constituent assembly and perennially served as a senator.² My maternal grandfather, who had been an Ottoman officer in the First World War, was the first superintendent of the Iraqi military academy in the 1920s. He lasted only nine months as superintendent, however, because the defense minister, Jafar Pasha al-Askari, who was one of the founders of the modern state of Iraq, appointed a British “advisor” to the academy and my grandfather resigned. He despised the British: he had fought against them in the war and didn’t want to be associated with a British advisor. Then he was elected to the first Chamber of Deputies, the lower house of Parliament, where he served for a time. My paternal grandfather served in the Senate and then became the inspector general of the Iraqi Ministry of Education. My father’s first cousin, an

economist, was the minister of development in the 1940s and 1950s. So I come from a line of political figures and academics.³

WHITESIDE: Does your family have any particular tribal affiliation?

AL-ISTRABADI: We are not a tribe; al-Istrabadi is a family name. We’ve been in Baghdad for seven centuries. The story is that we’re De’zei on my mother’s side, which would make us Kurdish. My maternal grandfather was mostly Kurdish, although his mother was Arab. Whether you have lived in Iraq’s cities, as my family has for centuries, or in the tribal areas, we’re all highly intermarried, and I have Arab, Kurdish, Persian, and Turkman blood. Also, my father’s family are Shi’a and my mother’s family are Sunni. This is very common in Iraq.

WHITESIDE: In a professional military education course that I help teach at NPS, we have our students participate in a US National Security Council simulation. We try to give the students a current crisis to study, so they can see what it’s like to make decisions based on the same limited information that policy makers have. The topic we gave them this quarter (early 2020) was the looming confrontation between the United States and Iran. One thing that the students struggled with was how to deter Iran from killing American soldiers, citizens, and contractors, such as the Iraqi-American who was killed in late December near Kirkuk. The students developed options in the simulation for a fictional president, but expressed little confidence that their ideas would work in the long run.

AL-ISTRABADI: With regard to the killing of Qassem Soleimani [commander of the Iranian Quds Force], the fears of imminent attack that were put forward as a legal justification for the killing appeared to dissipate, mostly for logical reasons.⁴ If an attack were imminent, you would not prevent that attack by decapitation. You would prevent an imminent attack by engaging with the force that was about to attack you before it actually attacked you. So that was always a hollow justification from a legal point of view. The only justification left is the notion that Soleimani’s death would deter the Iranians. I think that that is a vain hope because we’ve seen that in fact there was an immediate Iranian response.

I favored entering the Joint Comprehensive Plan of Action [JCPOA, commonly known as the Iran Nuclear Deal] at the time, and I still think that withdrawing from it was a mistake.⁵ I think the Obama administration would have done much better [than the current administration] in

engaging the Iranians diplomatically in other matters, as well. That would have been politically wise for the Iranians internally—assuming it succeeded—because such engagement would have addressed some of the criticism that was aimed at the Iranian leadership. The Iranians would have had an incentive to deal on some of the larger issues at least, such as refraining from either a direct confrontation with the United States or a proxy confrontation, and avoiding the targeting of US assets in the region. As it is, the United States chose to escalate with Iran, apparently without having a clear strategic objective, and then it became an exchange of tit-for-tat responses. What was the strategic imperative and what was the strategic advantage for the United States in targeting Soleimani? I don't question the legality of targeting him, but I do question the strategic value in having done so. What was gained?

WHITESIDE: Moreover, there is the problem of killing him inside Iraq.

AL-ISTRABADI: That was clearly and simply the wrong time and the wrong place. They could have done it a couple hours earlier, or over the deserts of Syria, and had some plausible deniability by claiming that it was a mechanical failure or whatever. That would have been one thing, but to have done it in Iraq, with Iraqi officials in the motorcade... Not that I'm weeping any tears for Abu Mahdi al-Muhandis, but his death created complications domestically within the Iraqi polity and also for the United States in terms of this clash between the United States and Iran.⁶ I think diplomacy is a good thing, and I don't see any sort of US diplomatic effort or plan. In fact, the [Trump] administration is gutting the US diplomatic corps. I don't see any direction for US

A strong defense and a credible military deterrent have to be supported by strong diplomacy.

President Obama speaks on Iran Nuclear Deal.



diplomacy to go with regard to Iran. That track seems to be wholly absent, and in its absence, I don't know what might be a good deterrent. I don't think the targeting of senior Iranian officials is going to be much of a deterrent, so I fundamentally don't see a way out.

WHITESIDE: That's what the students in the NSC classroom simulation said. They could not solve this policy problem.

AL-ISTRABADI: The only way forward is to engage diplomatically. The problem is that President Trump ratcheted up the tension so much. It's interesting to see, because he ratcheted it up and then he immediately gave the Swiss president his cell phone number to give to [Iranian President Hassan] Rouhani. He's begging the Iranians, "Call me." Well, why not talk to them before you withdraw from an agreement that they were already abiding by? The JCPOA had many flaws and it was a legitimate thing to say, let's see if we can improve the agreement and add another component, maybe expand on the strategic issues beyond the nuclear front. But simply to withdraw when the Iranians were abiding by it? What's their incentive to negotiate? The approach was, I think, wrong. While I obviously believe in having a strong defense and a credible military deterrent, these have to be supported by strong diplomacy. Because without that, as the old saying goes, if the only tool you have is a hammer, every problem looks like a nail.

IAN RICE: In 2016 and 2017, as the chief of the Tribal Engagement Coordination Cell at the US Embassy in Baghdad, my team and I strongly raised the alarm about the influence Iran was wielding through the al-Hashd al-Sha'abi [Popular Mobilization Forces, or PMF]. We considered trying to deter the Iranians by creating a wedge between the Iranian-backed al-Hashd al-Sha'abi and the Iraqi nationalists backed by Grand Ayatollah Sistani. In order to gain favor with the nationalists, the concept was for the United States to develop a relationship with the Sistani-backed militia groups and potentially provide them with security assistance, including training and materiel. The Sistani-backed militias are actually patriotic Iraqis looking to repair their state and defend their country, so it was an easy choice to develop a concept to support them and drive a wedge between them and the Iranian-backed proxies. The idea was to make the Sistani-backed groups into a patriotic example that could be emulated by the Iraqi populace and that would also set the militias apart from the Iranian groups. To accomplish this, however, required extensive negotiations with the various militia leaders and, because many were Iraqi nationalists, they were, understandably, anti-American. In your opinion, did

this idea have any legs in terms of diplomatic measures? The concept came from a junior foreign service officer, and it seemed to be the most reasonable suggestion for deterrence that we had at the time.

AL-ISTRABADI: That is a possible approach, although to succeed, it can't be seen by Iraqis as an American idea. The United States could support such an approach but you would have to find Iraqi interlocutors who would be the ones to actually advance that agenda, and then the United States can come in *quietly* in support—and without tweeting about it.

What we've had is this wholesale rape of the country by the political class in Iraq.

"Good governance" is a phrase we use whenever any problem arises, and I don't want to be Pollyanna-ish about this, but I do think that if Iraq had had good governance, if we had had successive governments that were less corrupt, that would have cured a lot of Iraq's ills. I'm not asking that the government be like Sweden, but maybe just Persian Gulf levels of corruption, where the elites and their children have really nice cars and nice second homes in London, but at the same time, they're building hospitals, schools, and roads in their home countries and allowing commerce, so that a rising tide can lift all boats. That's not ideal; I'd love to have the Swedish model of zero corruption but, realistically, I'm willing to tolerate some corruption in exchange for real services on the Gulf model. This, by the way, is what the Kurds are doing. There's corruption in Iraqi Kurdistan but, at least in Erbil, there's also building taking place, and some in Sulaymaniyah, too. I don't mean that as an endorsement of corruption, but what we've had is this wholesale rape of the country by the political class in Iraq and nothing is being invested. Good governance includes a political class that uses the state's assets to invest in the country, that encourages foreign investment and the development of a private sector. The current knee-jerk response of the Iraqi government whenever there are protests about lack of jobs and lack of opportunity is to find ways to hire more people in the government sector. I think our public sector payments are something like \$50 billion a year. That's simply not sustainable as an economic model.

The support that some of these militias have is in part because they pay their fighters. And now they're receiving government payments plus engaging in illicit activities, so they're getting paid from both sides. Take away that monetary incentive to fight or that need to illegally support militia leadership and maybe you can drive those sorts of wedges between them. The religious authority has

made a basic error—a *fundamental* mistake, for me—in justifying the PMF. I don't care what the Marajiyah [Shi'a religious authority] meant when it tried to claim that it didn't mean to set up private militias, but meant people should go volunteer for the army or the police force. But it was too late by then. Abu-Mahdi al-Muhandis of Kata'ib Hezbollah and Hadi al-Amiri of Badr and Qais al-Khazali of Asa'ib Ahl al-Haq had already been off and running, conducting operations well before Iraq's central government had established any control over them. So, Iraq has established these non-state actors on an equal footing with the state, on the Hezbollah model. Has anyone figured out how to deal with Hezbollah? Because if you figure that out, you'll be able to figure out what to do in Iraq. It's a very complicated problem.

RICE: Yes, we had experiences with some of the USAID [United States Agency for International Development]-funded NGOs [non-governmental organizations] in western Ninewa. They commented regularly that they worked with Kata'ib Hezbollah. This is the Lebanese Hezbollah model: use somebody else's money to obtain and to provide services. That's what Kata'ib Hezbollah was doing: getting someone to provide services for its operations. And we, Americans who were examining this issue, believed

Nthis was the case because Kata'ib Hezbollah and other Iranian-backed groups had Lebanese Hezbollah advisors in addition to Iranian advisors.

AL-ISTRABADI: I remember having this discussion with an American ambassador back in 2006, when I was still in New York. There was a war between Israel and Hezbollah, and she was saying, "These [Hezbollah] are terrorists." I said, "I understand from your perspective and, maybe, from mine, that these are a bunch of terrorists, but look at it from the Lebanese perspective. The Israeli army bombs your village in Lebanon and destroys your house. The next day, a Hezbollah representative comes with \$25,000 in cash—and this is \$25,000 in some village in Lebanon, not in Manhattan where you can't buy a brick for \$25,000—for you to rebuild your home. Whose side are you going to be on?" And she said, "Well, that's all Iranian money." I answered, "Do you think you'd care where the money came from?" So, I really think our policy makers think about these problems from the wrong perspective.

RICE: Another great example of this was the fact that the Iranian-backed militias didn't have any of the same vetting requirements that the Iraqi government-funded militias had to meet to bring in Sunni fighters. If you were an

President Donald J. Trump signs a National Security Presidential Memorandum as he announces the withdrawal of the United States from the Iran Nuclear Deal.



Iranian-backed militia, you could just give a Sunni fighter in Ninewa \$500 a month, a gun, and a car. And that was all fine. If your militia was supported by Ninewa province's mobilization committee and trained by Americans, then, oh my goodness, you had to go through all these gates to hire fighters, and it wasn't even fair in terms of seeing the comparative advantage. I mean, if Kata'ib Hezbollah shows up at your doorstep and says, "Hey I'll give you two choices: I'll burn you out or I'll give you \$500, a weapon, and a car," well, it's a pretty easy choice.

AL-ISTRABADI: I remember talking to [Coalition Provisional Authority chief Paul] Bremer, at the time when the [anti-coalition] insurgency was getting going. People were already talking about the "Sunni triangle," and I said "You know, Ambassador Bremer, the tribes and the tribal leaders didn't love Saddam Hussein; he bought their loyalty with cash and brand new Chevy Suburbans," and Bremer said, "We don't do things that way." Well, when [Commander of the Multinational Forces in Iraq General David] Petraeus and [US Ambassador to Iraq Ryan] Crocker were in Baghdad, that's *exactly* what they did.

WHITESIDE: To reinforce your point, I myself [as a representative of the US government] paid Sunni tribal auxiliaries in the south of Baghdad during the Surge in 2007. So, do you think this conflict between the United States and Iran in Iraq was always inevitable once the so-called Islamic State was defeated, at least militarily and politically? And are the Iranians, who, at least according to their narrative, pushed the United States out once before in 2011 and aim to repeat that feat again, going to pull this off?

AL-ISTRABADI: No. You have to remember the history of these relationships. I want to say, "defeated" is a relative term. ISIS is obviously not destroyed.

WHITESIDE: Defeat as a temporary condition?

AL-ISTRABADI: Precisely my point. ISIS is obviously reconstituting itself. I co-edited the book *The Future Of ISIS: Regional and International Implications* and wrote a chapter in which I talked about how ISIS would inevitably lose the territory they controlled and transform into a more traditional terrorist organization that launches the occasional spectacular event.⁷ I think they're headed in that direction. You have to remember that it was exactly when ISIS was defeated that the United States withdrew from the JCPOA. Which was, from an Iraqi perspective, exactly the wrong moment.

WHITESIDE: Is it your understanding that the most important factor influencing a future rise of ISIS is the US decision to opt out of the nuclear agreement with Iran, and the subsequent tensions between the two countries that would give room for the group to regain strength?

AL-ISTRABADI: Iraq had finally regained—at a horrible cost, particularly for the locals, for Mosul, for Tikrit—Iraqi territory, and believed it was the time to think about reconstruction. What we needed was a ratcheting *down* of the tensions between the United States and Iran, so that the stakes wouldn't be so high for Iran to give the Iraqi political class, inferior as it is, the opportunity to think about what a post-ISIS Iraq should look like. By the way, this is one of my critiques of Brett McGurk [former US Special Presidential Envoy for the Global Coalition to Defeat ISIS from 2015–2018], who, in my opinion, spent zero time thinking about what a post-ISIS Iraq would look like. Although he's not military, but as much of a civilian as I am, he was focused like a laser beam on liberating the next square meter of Iraqi territory, which isn't his business. I mean that in the literal sense: that is a military function. He ignored what should have been his work as a diplomat. The military was going to coordinate how we were going to get Iraqi territory liberated. McGurk's function was to figure out how to help create a stable polity that wouldn't descend again into the same nonsense that led to the rise of ISIS in the first place. In my judgement, he spent zero time thinking about that. His whole plan was that we'd liberate Iraq from ISIS and Haider al-Abadi would run for prime minister again and, because he would be seen as the liberator of Iraq, he'd be reelected. But it didn't work that way because, whatever the facts are, the media narrative was that Hadi al-Amiri [the leader of Iraq's Iranian-influenced Popular Mobilization Forces] was the great liberator of Iraq, not al-Abadi.

RICE: When I was talking to one of McGurk's advisors in 2017, I said we still have a chance to avoid turning over all the successes we have made in the counter-Islamic State campaign to the Iranians if we recognize that, with every airstrike that the US-led coalition brings to bear on ISIS, the Iranian-backed PMF militias are seizing the ground without competition. The answer was simply, "Sorry, but that's the strategy." The Inherent Resolve campaign to liberate Mosul and defeat ISIS had to be completed within a two-year US election cycle.

AL-ISTRABADI: I think my article in 2009 actually said this same thing.⁸ Unfortunately, the United States is never more than two years away from an election, and that's been its policy in Iraq since 2003: we have to get *this* done

because we have a congressional off-year election; we have to get *this* done because we've got the president's reelection; we've got to get *that* done because we've got another damned—pardon me—congressional election, etc.

A lot of these tribes in Ninewa wanted to mobilize because they are deathly afraid of the Iranian-backed militias.

RICE: It's interesting that you bring this up, because the various US and coalition leaders that I met with would have the same discussions on the lack of strategy—even beyond the immediate military objective—for a bridging objective to avoid disenfranchising the Sunni population. Because that is clearly what we are now seeing. The reason a lot of these tribes in Ninewa wanted to mobilize is because they are deathly afraid of the Iranian-backed militias.

AL-ISTRABADI: Well, they have good reason to be.

RICE: But then, there are also some very non-altruistic motives. Specifically, there were social-class elites who wanted access to political power and economic opportunities. They also wanted to manage the revenge against former ISIS members. On the one hand, these leaders wanted to eliminate or exile former ISIS members. On the other hand, some leaders wanted to pardon them. In the vacuum of ISIS's defeat, these elites were going to come in and do certain things such as change the balance of political, social, and economic power in local areas. To follow up on the point you brought up about corruption, the United States conditioned the Iraqis to favor corruption over good governance. I can't even tell you how many of my partners just wanted income streams and contracts. And that's the primary reason why they wanted the Americans to stay in Iraq.

AL-ISTRABADI: Look back at the CPA [Coalition Provisional Authority], and how many tons of hundred-dollar bills came up missing? And you want to talk about conditioning? I will say they were modeling corrupt behaviors. How many no-bid contracts were led by the CPA? How many friends of [then-Vice President] Dick Cheney got contracts? This is a point that I have talked about in my academic life: imperial powers govern in the peripheries very differently from how they govern in their main cities. Thus, the United States modeled corrupt practices for the Iraqis. Not to say that our political class needed much tutoring in that but, nonetheless, it didn't help.



Vice president of Iraq Tariq al-Hashimi

Also with regard to good governance, what price did [Iraqi Prime Minister] Nouri al-Maliki pay for targeting the sitting vice president of Iraq [Tariq al-Hashimi] on terrorism charges? I don't know whether al-Hashimi did the things he was accused of, and I have absolutely no brief to defend him, but the convictions were based on confessions and one of his guards died during the investigation. The Obama Administration's response, thanks to Brett McGurk, was that this was a domestic Iraqi issue so there was no price for Maliki to pay for engaging in these practices.

US policy has consistently been, “Who are we for?” rather than “What are we for?” And so US policy will continue to fail in Iraq.

He also didn't pay a price for sending troops loyal to him directly into Fallujah and Ramadi in 2013 to break up what were largely peaceable demonstrations, which were having absolutely no impact in Baghdad anyway. He did it to show that he was tough. In 2012, there was a constitutional process in parliament to withdraw confidence in Maliki, which had never happened before in Iraq's history. We're on our fourth or fifth incarnation of the Republican Era, and no government has ever fallen to such a vote in parliament. We were on the verge of that. What a precedent for constitutional governance that would have been! But as the leader of the opposition said, “I can resist American pressure and I can resist Iranian pressure, but I can't resist American and Iranian pressure.” So, although a vote of no confidence was his idea, he was the first person to withdraw his bloc's votes, and then the whole effort collapsed. That became, in my opinion, the proximate cause for the rise of ISIS two years later. The lesson that Maliki learned was that he could get away with anything. US policy has consistently been, “*Who* are we for?” rather

than “*What are we for?*” And so US policy will continue to fail in Iraq.

WHITESIDE: Can the legal and political integration of the PMF into the Iraqi government be undone in any way?

AL-ISTRABADI: Practically speaking, it’s very difficult, because they weren’t truly integrated [into national security forces]. They were formally integrated and they’re on a government paycheck, but they were integrated whole, as discrete units with their own command structure. And, to my knowledge, they report directly, officially, to the prime minister rather than through the legal chain of [military] command. That’s actually one of the flaws of the Iraqi constitution. It says that the prime minister is the commander in chief, but it doesn’t say what that means. The South African constitution says the same thing, and runs on for five pages about what it means for the president to be the commander in chief. But with that line in Iraq’s constitution being as vague as it is, prime ministers can do whatever the hell they want to and technically they’re complying with the constitution. It’s a huge flaw. There’s a legal chain of command in the enabling statutes but, of course, a constitutional provision trumps the statutes.

WHITESIDE: Are there alternative ways for the United States to support a counter-ISIS campaign that would be less intrusive and accommodate Iraqi desires for much less overt American influence, now that ISIS is not an immediate serious political threat? Is there room for such a shift, especially from a combating terrorism perspective? Or are you more worried that this will go to extremes?

AL-ISTRABADI: If you remember the famous *Atlantic* interview of Obama and some of his officials by Jeff Goldberg, even the Obama administration’s thinking about Syria at the time was: do nothing or [repeat the Vietnam experience]; do nothing or [repeat the Iraq invasion and occupation of 2003–11].⁹ Vladimir Putin has proven fairly well that you can intervene militarily in a limited way and achieve your strategic objective without putting 150,000 troops on the ground. I’m not condoning the manner in which the Russian air force conducts its operations, indifferent as it is to civilian casualties and unafraid to do anything at all. I understand that no American commander would tolerate that kind of approach to war, and I support that.

There was clearly some spectrum of intermediate approaches the United States could have implemented between zero and another Iraq and Syria. Now saying that, that has to be true of Iraq’s approach as well. Continued

security cooperation between Iraq and the United States, including continued training and intelligence sharing, is in the interest of both Iraq and the United States, and I gather that the Iraqi government has recently resumed [limited] counter-ISIS operations with the United States, since the assassination of Qassem Soleimani.¹⁰ One of the mistakes that occurred in 2011 was the withdrawal of intelligence cooperation. I am told that it crashed virtually to zero when the United States decided to completely withdraw military forces in 2009.

RICE: I suspect that is true, but I believe we maintained advisors with the Counter-Terrorism Service from 2011 to 2014, when the United States returned in support of Iraq’s central government to defeat ISIS.

AL-ISTRABADI: In any case, the intelligence exchange was inadequate. McGurk says—and I have no reason to think it’s not true—that in the three or four days before Mosul fell, he actually warned Maliki that ISIS was getting ready to surge back into Iraq and that Maliki dismissed the notion. Obviously, there was a loss of trust between Maliki and Americans like McGurk on the ground. McGurk has also said that even [Kurdish President Masoud] Barzani was getting hints in Erbil of what was coming. Maybe none of that is true, but that’s what he testified to.

WHITESIDE: I don’t think much of that is true, from what I’ve seen in my research of the Islamic State’s military campaign in Iraq before 2014. The ISIS campaign in Iraq was substantial, if not operating at a very high level, as early as 2012 if not before. The attack data show that Mosul was under severe stress in 2012 averaging 10 attacks a day. We were missing that. You’re correct to say that the United States either didn’t synthesize that information correctly or didn’t pass it on to trusted partners. I think the Iraqis also knew, but the reporting chain up to Maliki was damaged because of political issues [mainly because Maliki made political appointments of generals in the security forces who were loyal to him but not necessarily the best choice for the job].

RICE: My research focuses on external patrons and local clients. Iraq’s constitution seems to be a great example of how external patrons can influence the way a government is formed while a country is being occupied. Who was the prime driver in the writing of the constitution: Americans, external patrons, the British, or the UN? Also, what were the frictions that influenced the process?

AL-ISTRABADI: I wrote about this in my 2009 article [“A Constitution Without Constitutionalism: Reflections on

Iraq's Failed Constitutional Process" (see note 8)]. The Americans didn't really care what Iraq's constitution said. They needed a constitution [pounding hand on table]! Because we're gonna have elections here [loud pounding]! And someone needed to be able to say, "Look at the progress we're having in Iraq." Sheikh Humam Hamoudi was the chairman of the drafting committee. The TAL [Transitional Administrative Law] also provided for two possible delay mechanisms in the drafting of a permanent constitution: one would extend the drafting time by six months without triggering new elections, and the other would mandate elections in the face of an impasse or the failure of the constitutional referendum. In that case, the one-year drafting deadline would be renewed.

The TAL, the interim constitution, took longer to draft than the permanent constitution of Iraq. As I remember, we took about four months to draft the TAL. Work on the permanent constitution took less than five weeks. A consequence of that speed is that there is not even a provision for the resignation of a prime minister in the constitution, an event that occurred on the twenty-ninth of November 2019.¹¹

Sheikh Hamoudi asked for a 30-day extension under the six-month provision of the TAL, but before anyone in the Iraqi political class responded to him, Zalmay Khalilzad, the US ambassador to Iraq, said, "The Iraqis don't need any more time. There will be no extension." So our timetable was an American timetable.

Now, you wanted to ask about the content of the constitution. The Americans didn't care what was in it, as long as they could say, in the 2006 US off-year elections, that it was done. So we fought tooth and nail in the TAL to keep religious scholars off the constitutional court, and we succeeded. It was Ambassador Khalilzad who conceded to it in the final document. There were no Sunni interlocutors in the drafting process to speak of. They were locked out. The Kurds didn't care because they knew that under the idiotic federalism provision, they could basically annul any law they didn't like, with very limited exceptions such as foreign policy and national defense. So they didn't care what was in the final document, and they weren't going to infuriate the Shi'a religious party over this. So there was nobody to say, Wait a minute, damn it, you're dismantling the civil state of Iraq! Khalilzad wrote an op-ed that justified this provision, saying that if Islam is going to be a source of law, then of course you have to have religious scholars on the court. Well, Islam has been the source of law of every Arab country since the end of the Ottoman Empire, but it doesn't mean we have to have religious scholars on our courts! I'm sorry I'm getting angry about



Zalmay Khalilzad

this—it's the ignorance and the arrogance of the officials that we have to deal with. I dealt with Khalilzad before I went to New York, and then again briefly while we were both in New York before I left. The arrogance was incredible.

If you look at the Iraqi constitution, it is a description of the fears of each community.

And if you look at the Iraqi constitution, it is a description of the fears of each community, mostly the Kurds and the Shi'a. There is nothing in the constitution that unites the Iraqis as such. The concepts of nationality, of nationhood, of belonging, do not exist in it. And the Americans didn't care; they needed the constitution on a timetable. In the meantime, I have the Marajiyah ratcheting up its demands to increase the Islamization of the constitution and of the state. Now it has backpedaled on this because the constitution has been a spectacular failure. So now I have the Marajiyah in Najaf, Ayatollah al-Sistani's office, calling for a civil state. Well, where the hell were you fifteen years ago? And what, by the way, does a civil state mean to the Grand Ayatollah al-Sistani? Does it mean the same thing that it meant to me? I have my doubts. Or is it just a slogan, because that's where the Iraqi youth in the street are headed? They want a civil state. Nowhere in the constitution does it mention *al-muwatin*, which may be translated as "citizen." A sectarian division of spoils does not appear anywhere the constitution, but it is promoted indirectly by inclusion of the *aza al-Husayn*—Husayni practices [Shi'a mourning rituals for Husayn, the slain grandson of the Prophet, killed at the Battle of Karbala in 680 CE]. I don't know how you translate it—the rituals that are associated with self-harm [*tatbir*, or self-flagellation, is a customary act during Ashura celebrations]. That's in the Iraqi constitution, for God's sake!

So, the Iraqi constitution is far from attempting to form a more perfect union. It codifies the disunion of Iraq. And that was the work of the Iraqis. If you want me to say the Iraqis did this, they didn't!

RICE: I'm interested in external patrons and local clients, as we just discussed. I think it's obvious that the lack of a civil state decreased the certainty on the Iraqi street, decreased the certainty of day-to-day life because people didn't feel as if they were citizens. There was a disunion.

AL-ISTRABADI: It's not that the rank and file didn't feel like citizens. It was the political elite who had returned from exile. There's a huge distinction between those two groups. The constitution was written, from a Shi'a religious perspective, as a hedge against what was, specifically in the view of the supreme council, a Sunni return to power. Now, by the way, I reject the notion that the Sunnis were running Iraq under Saddam Hussain. *Saddam Hussain* ran Iraq! He happened to be from Tikrit, the Sunni part of Iraq. The Sunni people weren't running a goddamned thing in Iraq but that was the narrative, and Sunni equals Ba'athist. So the constitution was a hedge against a Ba'athist return to power.

INTERVIEW TEAM: Thank you for helping us understand the complexities of the Iraqi-US strategic relationship and our rivalry with Iran in Iraq, and the evolution of current Iraqi politics. We appreciate your time, Mr. Ambassador.

ABOUT THE AUTHORS

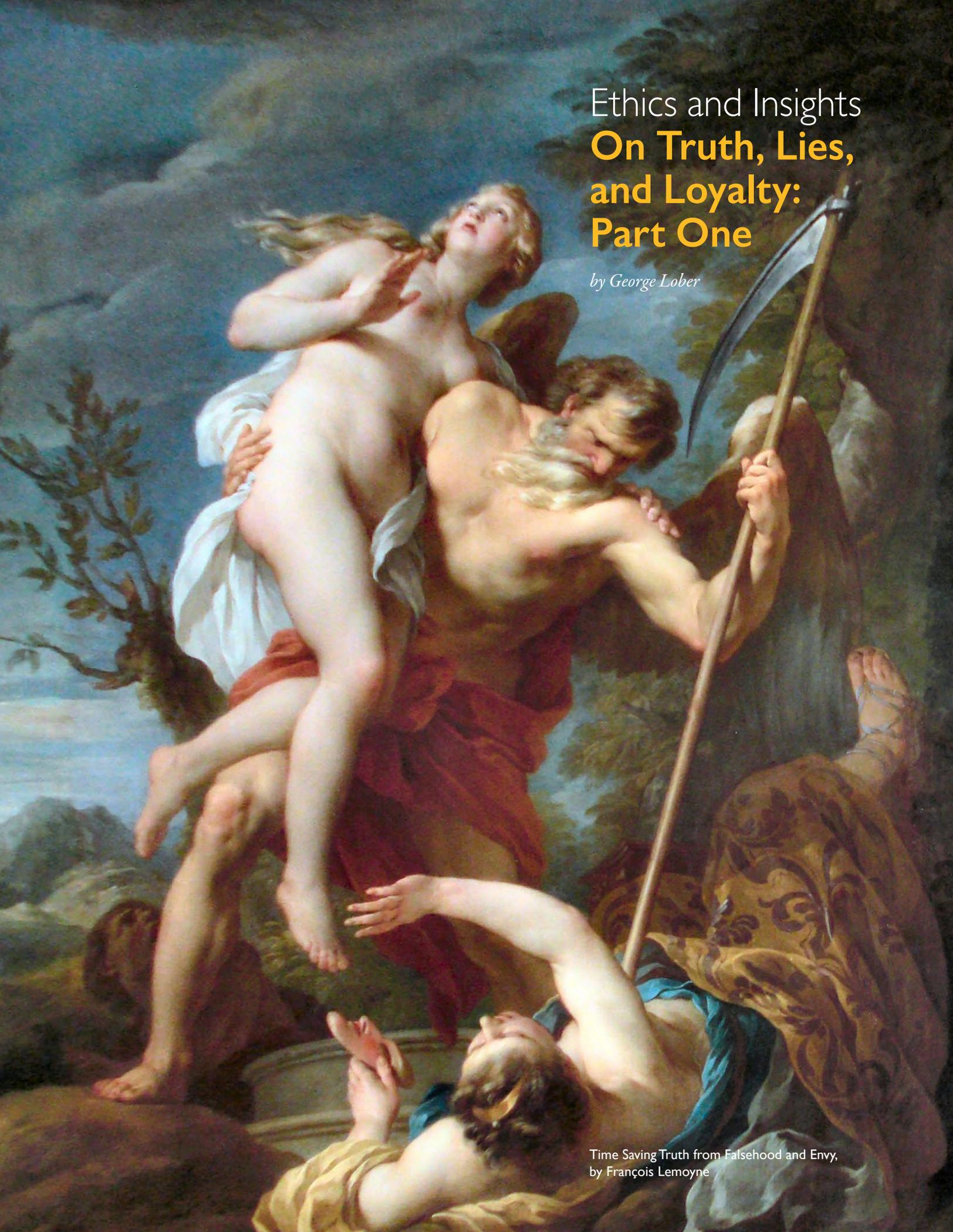
Dr. Craig Whiteside is a professor of theater security decision making for the Naval War College Monterey.

COL Ian Rice is a retired US military officer.

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 interview was edited for length and clarity. Text inside brackets was added by the editorial team. Every effort was made to ensure that the meaning and intention of the participants were not altered in any way. The ideas and opinions of all participants are theirs alone and do not represent the official positions of the US Naval Postgraduate School, the US Department of Defense, the US government, or any other official entity.
2. Al-Hajj Mahmoud al-Istrabadi was one of the drafters of Iraq's first constitution in 1925.
3. Ambassador al-Istrabadi's paternal grandmother, Bibiya al-Istrabadi, unsuccessfully tried to help smuggle Nuri al-Said, Iraq's long-serving prime minister, out of Baghdad during the 1958 coup that deposed Feisal II, the British-installed Hashemite monarch. When they were discovered, both Bibiya al-Istrabadi and Nuri al-Said were killed; in a seminal event in Iraqi history, Nuri al-Said's body was brutalized by his fellow citizens. See Aram Roston, *The Man Who Pushed America to War: The Extraordinary Life, Adventures, and Obsessions of Ahmad Chalabi* (New York: Nation Books, 2008).
4. Soleimani was killed in a US drone attack on 3 January 2020 as he was leaving the Baghdad airport. See "Qasem Soleimani: US Kills Top Iranian General in Baghdad Air Strike," BBC News, 3 January 2020: <https://www.bbc.com/news/world-middle-east-50979463>
5. The Joint Comprehensive Plan of Action (JCPOA) went into effect on 16 January 2016, after two years of negotiations between the United States, Iran, France, Germany, China, Russia, the European Union, and the United Kingdom (then still part of the European Union). Despite verification of Iran's compliance with the terms of the agreement, the Trump administration withdrew the United States from the JCPOA in May 2018.
6. Abu Mahdi al-Muhandis was the *nom de guerre* of Jamal Jaafar al-Ibrahimi, a key leader of the Iraqi Shi'a Popular Mobilization Forces. He was killed alongside Soleimani in the US drone strike on 3 January 2020.
7. Feisal al-Istrabadi, "Regional Constraints on the U.S. Confrontation of ISIS," in *The Future of ISIS: Regional and International Implications*, Sumit Ganguly and Feisal al-Istrabadi, eds. (Washington, DC: Brookings Institution Press, June 2018): <https://www.brookings.edu/book/the-future-of-isis/>
8. Feisal al-Istrabadi, "A Constitution Without Constitutionalism: Reflections on Iraq's Failed Constitutional Process" *Texas Law Review* 87 (2009), available at Articles by Maurer Faculty, 2362: <https://www.repository.law.indiana.edu/facpub/2362/>
9. Jeffrey Goldberg, "The Obama Doctrine," *The Atlantic*, April 2016: <https://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/>
10. Alissa J. Rubin and Eric Schmitt, "U.S. Military Resumes Joint Operations with Iraq," *New York Times*, 15 January 2020.
11. Prime Minister Adel Abdul Mahdi submitted his resignation to the Iraqi parliament on 29 November 2019 following violent anti-government protests. See Arwa Ibrahim, "Uncertainty Remains as Iraq Parliament Accepts PM's Resignation," Al Jazeera, 2 December 2019: <https://www.aljazeera.com/news/2019/12/iraq-pm-offer-quit-country-191201092331173.html>



Ethics and Insights
**On Truth, Lies,
and Loyalty:**
Part One

by George Lober

Time Saving Truth from Falsehood and Envy,
by François Lemoyne

AS I WRITE THIS, IN THE SPRING OF 2020, I am living through the third month of California’s state-wide shelter-in-place order to control the spread of the novel coronavirus. My neighbor remains convinced that measures to control the coronavirus pandemic are part of a political plot by persons nefarious and unidentified. The online film *Plandemic* continues to spread like, well, a virus, despite widespread debunking of its incendiary claims and the responsible efforts of both YouTube and Facebook to take it down. The hashtag *#virustruth* continues to spin the conspiratorial theory that the pandemic is part of a plot by elites with unspecified motives to initiate a third world war. To borrow a phrase from Stevie Wonder, it’s starting to feel like Truth’s in need of love today.

Case in point: I recently received an email from a military officer and former student from Africa. I had written him earlier in the month, asking how he and his family were faring with the COVID-19 pandemic, and how the virus was affecting his country. When he replied, he assured me that both he and his family were well and doing all they could to remain so, including wearing masks, using sanitizers, and washing their hands often. However, his country, he said, was not coping as well; the virus was just beginning to strike hard and the number of deaths was rising. He offered two specific reasons why this was so: his country possesses a weak, under-equipped healthcare system, and the population does not believe in the seriousness of the threat. The former reason did not surprise me; after all, his country is among the poorest in the world. However, the latter reason, a distrusting population, struck me as one more indicator of a growing assault on Truth—and by extension, Trust—around the world.

In response to my student’s email, I found myself thinking about two writers: the philosophers Harry Frankfurt and Sissela Bok. Although they’re starkly different from each other in most respects, they share a common view of the importance of Truth.

Frankfurt first published his small book *On Truth* in 2006, as a sequel to his 2005 national bestselling essay, *On Bullshit*. In *On Truth*, he offers a quick summary of the earlier piece, including a working definition of “bullshit” as the tool of choice for individuals “who are attempting by what they say to manipulate the opinions and the attitudes of those to whom they speak.”¹ Such manipulators, he suggests, focus solely on “whether what they say is effective in accomplishing this manipulation. Correspondingly, they are more or less indifferent to whether what they say is true or whether it is false.”² I have no idea whether Frankfurt foresaw our current post-truth, alternative facts, fake

news world of conspiracy theories and deliberate misinformation and disinformation, or whether he was simply reacting to current trends as he saw them. In either case, he obviously recognized the “extraordinary prevalence and persistence”³ of such manipulative efforts in American culture at the time, and he offered the strong opinion that “bullshitting constitutes a more insidious threat than lying does to the conduct of civilized life.”⁴

“Truth often possesses very considerable practical utility.”

Shortly after *On Bullshit* was published, however, Frankfurt realized he had committed a serious philosophical omission: he had taken for granted that his readers would automatically agree on “exactly why truth actually is so important to us, or why we should especially care about it.”⁵ He subsequently wrote *On Truth* to advocate that “truth often possesses very considerable practical utility.”⁶ He further suggested that any society that hopes to continue to exist must have “a robust appreciation of the endlessly protean utility of truth.”⁷ To drive the point home, he asks,

After all, how could a society that cared too little for truth make sufficiently well-informed judgments and decisions concerning the most suitable disposition of its public business? How could it possibly flourish, or even survive, without knowing enough about relevant facts to pursue its ambitions successfully and to cope prudently and effectively with its problems?⁸

Frankfurt published *On Bullshit* in 2005 and its sequel *On Truth* in 2006.





US President Bill Clinton and Monica Lewinsky

By comparison, Sissela Bok first published her expansive study, *Lying: Moral Choice in Public and Private Life*, in 1978, revised it in 1989, and then revised it again in 1999, following the scandal involving US President Bill Clinton and a young White House intern named Monica Lewinsky. In *Lying*, Bok undertakes a moral examination of the pernicious and manipulative nature of lying. She considers a spectrum of circumstance, from personal crises to deceiving the public for its own good, under which lying may occur. In doing so, she carefully defines a lie as a statement known to the liar to be false and intended to deceive and manipulate the perceptions of the one being lied to.⁹ She then identifies at least two fundamentally unethical and potentially dangerous aspects of lying and, by implication, highlights the moral importance of telling the truth.

First, she argues, lies are corrosive to the social fabric. In that regard, she agrees with Frankfurt that “some level of truthfulness has always been seen as essential to human society, no matter how deficient the observance of other moral principles.”¹⁰ To support this assertion, she alludes to the eighteenth-century literary figure, Samuel Johnson, and his observation that “even the devils themselves . . . do not lie to one another, since the society of Hell could not subsist without truth any more than others.”¹¹ The bottom line, Bok suggests, is that any society, even in Hell, will collapse when truth becomes indistinguishable from fiction.

As with Frankfurt, I have no knowledge of whether Bok consciously anticipated a world in which the “2020 Edelman Trust Barometer” would report that in a majority of the countries surveyed, “less than half of the mass population trust their institutions to do what is right,”¹² or a time in which the 2019 Pew Research Center Report *Trust and Distrust in America* would assert that “Americans

For Bok, any deception resulting from the manipulation of another is essentially a coercive act.

admit they at times have trouble distinguishing the truth from falsehood from certain sources.”¹³ It’s worth noting that both of those reports were prepared *before* the pandemic. But I do know that Bok understood the unethical and corrosive costs of using lies to manipulate the perceptions of others, whether members of society as a whole or specific individuals.

For Bok, any deception resulting from the manipulation of another is essentially a coercive act because “when it succeeds, it can give power to the deceiver—power that all who suffer the consequences of lies would not wish to abdicate.”¹⁴ Simply put, she claims that the liar invokes a power over the receiver of the lie that alters the latter’s perception of what is, or was, or will be, and that this power is one the victim of the lie would likely never knowingly grant. And that power, she insists, is essentially the same as any other means of coercion, in that the intent of the lie is to influence another to act in ways he or she would not otherwise choose and that are likely not in the victim’s best interests.

It’s that same power, Bok contends, that constitutes the second unethical aspect of lies based on deception and manipulation. At the purely personal level, a lie can dramatically impact the one lied to, “since we, when lied to, have no way to judge which lies are the trivial ones, and since we have no confidence that liars will restrict themselves to just such trivial lies, the perspective of the deceived leads us to be wary of all deception.”¹⁵ In other words, she cautions, once bitten, forever shy.

Lying by Sissela Bok



As a second case in point, consider another former student of mine—let’s call him Felix—who unexpectedly stopped by my campus office one summer day after graduating the quarter before. I was surprised to see him, but also delighted. He had been a joy to have in my ethics class: intelligent, funny, and always willing to participate. He knocked on my office door, asked if he could come in, and, when I said yes, entered and closed the door behind him. He sat in a chair by my desk, asked if I had a moment to talk, and, when I again said yes, immediately began to tell the story of how he had met a local woman during his studies at my school. The two of them, he said, had fallen deeply in love. At the time, he was a newly pinned captain in an elite government security unit; she was a rising executive in a start-up tech company. After almost a year of dating, he was planning to ask her to marry him, but he felt he owed it to her to be fully truthful and explain in more specific detail what his job entailed. Up until that time, he had been deliberately vague. So he shared with her the fact that his position occasionally required him to go undercover and assume another identity. In that assumed role, he then would manipulate and deceive other individuals to act in ways that were not always in their own best interests, although those actions may have been in the best interest of either law enforcement or the government. While undercover, he explained, he might not be able to contact her and, what is more, he often wouldn’t even be able to tell her when he would come home. He hoped she’d understand, see his work as patriotic, brave, and heroic, and trust in the strength of the love he had shown for her over the past year.

Unfortunately, she didn’t see it that way. Instead of accepting his plea for trust, she reacted with shock and fear. If his job and training required him to lie and manipulate others, she asked, how could she trust that he wouldn’t ever manipulate her? She’d been lied to by lovers before and she didn’t want to go through that again. How could she know he wasn’t lying and deceiving her right then? How could she trust his words? Felix assured her he was telling the truth and that his love for her was sincere, but she couldn’t cross that bridge. A few days later, she broke off their relationship and Felix was devastated. He was being truthful and hoped that she would believe him, while she was trying to protect herself and avoid once again being manipulated and deceived by someone who claimed to love her. In the end, she couldn’t escape her distrust.

At the end of his story, Felix looked at me and asked what I thought he could do to change the woman’s mind. I knew that the answer was “not much.” I offered some consoling support, and suggested that in time he might find someone

equally enchanting and deserving of his excellent character. I knew, however, that for some situations there are no easy answers, and that Sissela Bok was right. Lies aren’t only corrosive to society; they eat at the hearts of the ones lied to.

In fairness to Bok, though, I must add that she is not an absolutist; she concedes that not all lies are evil and that truth, obviously, is not always without cruelty. She does not insist that the truth be told and damn the consequences. In fact, with reference to “white” lies, she declares that

to say that white lies should be kept at a minimum is not to endorse the telling of truths to all comers. Silence and discretion, respect for the privacy and for the feelings of others must naturally govern what is spoken. The gossip one conveys and the malicious reports one spreads may be true without therefore being excusable. And the truth told in such a way as to wound may be unforgivably cruel, as when a physician answers a young man asking if he has cancer with a curt Yes as he leaves the room. He may not have lied, but he has failed in every professional duty of respect and concern for his patient.¹⁶

I agree with Bok. Not only can telling the truth in some situations be cruel, but I believe it can also carry high risk, particularly if the situation in question involves speaking truth to power. Neither Frankfurt or Bok addresses that dilemma, but I believe it merits its moment, if for no other reason than, as Steven Leonard writes,

in an environment where the people in positions of authority are willing and able to listen, the truth is a powerful change agent. In an environment where the people in positions of authority aren’t as willing to listen—or have no interest whatsoever in listening—the truth is an unwelcome intrusion and the consequences that come with speaking it can be brutal.¹⁷

That brutality can become abundantly clear within any organizational hierarchy. As the former management editor of the *Financial Times*, Gill Corkindale, affirms, “Bosses have many means to intimidate — by position, power, personality or even wealth and a sense of entitlement. And even if they do not openly intimidate, most executives expect and assume that employees will not question them and company policy, or, if they do, that they will go quietly.”¹⁸ Those employees or subordinates who

feel “impelled to speak up or ‘go public,’” she assures, “can be condemned for not being team-players or branded as troublemakers.”¹⁹

Employees or subordinates who feel “impelled to speak up or ‘go public’ can be condemned for not being team-players.”

Consider the case of a young, newly minted military officer, Jaime, who was selected to a special operations force and deployed to a platoon overseas. The platoon, based at an ally’s airfield, was under the command of a recognized hero within the force, a leader renowned for his bravery, patriotism, and integrity. Soon after Jaime arrived, however, he discovered that not everything in the platoon was on point. The once-heroic commander had developed an alcohol abuse problem and let his command of the platoon slip. Several members of the platoon, following the commander’s lead, were slacking in their duties and openly drinking during the workday. When Jaime learned that two members of the platoon had discharged their weapons at road signs in the local countryside, he became concerned enough to share his unease over the platoon’s morale with the senior enlisted officer, who listened and then advised Jaime to drop it. The commander, the chief told him, was aware of the behavior occurring within the platoon and didn’t see it as a loss of discipline. Nor, the chief added, did the platoon’s members, who understood all that the commander had gone through in his heroic career, perceive the commander’s behavior as a lack of leadership. And lastly, the chief assured him that the commander never appreciated receiving either advice or criticism from a junior officer as inexperienced as Jaime.

Whenever I reached this point in the story while teaching this case study to my ethics classes, I’d ask two questions: Does Jaime have a problem, and, if so, what should he do? Inevitably, there was no consensus among my students. Most answers regarding whether Jaime had a problem hinged on the degree to which he did, or did not, see his personal and professional principles aligned with the behavior of the platoon. If his principles aligned, then not a problem. If his principles did not align, but he valued his career in the force more than asserting what he believed to be right, then still not a problem, and Jaime could simply fall in line for the duration of the deployment. If, however, his principles did not align and he valued them more than he valued his career, then he had a big problem. As to what

Jaime should do in the last instance, the answers I heard from my students were always varied and complex.

According to Corkindale, the political economist Albert O. Hirschman identified the three most principled choices facing a civilian in Jaime’s position as “exit, voice, and loyalty.”²⁰ That person, Corkindale explains, can choose to

1. exit the situation via a formal principled letter of resignation;
2. voice one’s concerns by speaking truth to power and accept the consequences; or
3. remain and serve as a loyal team member.²¹

Unfortunately for Jaime, the matter of loyalty is not limited to the third choice alone, and for most people pursuing careers in homeland security and national defense, there are aspects of loyalty inherent in all three choices. In choice 1, Jaime’s paths to formally exiting his current assignment are complex and would force him to choose between loyalty to himself and his principles, loyalty to the members of his platoon, and loyalty to the larger force he serves. All such paths would likely require an explanation to higher-ups of his request for reassignment, and Jaime would have to confront the intersection of what the ethicist Rushworth Kidder calls the “truth vs. loyalty” ethical dilemma.²² Rather than remaining silent and loyal to the platoon, he could tell the truth about why he wanted to leave or he could lie, fabricate an excuse, and maintain his loyalty to the platoon while protecting his career. In choice 2, he could express his concerns directly to the commander, but if the commander’s response went as the NCO predicted, it’s quite likely the issue of loyalty would be raised and Jaime would have to declare his position going forward within the platoon one way or the other. Finally, in choice 3, Jaime could possibly feign loyalty to the platoon and remain in his position, but he would do so at the expense of loyalty to his own principles and ethics. Whatever Jaime’s choice, he would—as the French philosopher, Michel Foucault, cautioned—confront the inherent risks in speaking truth to such power.²³

Where does that leave us? To begin with, we have both Frankfurt and Bok telling us that lying is harmful to the moral fabric of society, that it fosters distrust and erodes the ability of a society to function. Add to their dark portent Frankfurt’s warning about the pernicious danger of bullshit as a similar threat to society, and Bok’s observation that lying is both insidious and unethical because the liar assumes a power over the one being lied to that the latter is both unaware of and likely would never have

willingly granted. By lying, the liar exercises the power to manipulate the victim of the lie as coercively as if he or she had used more overt efforts of control. And thus, we are left with the conclusion by both Frankfurt and Bok that truth is foundational to society and the individual.

I still believe in advocating for truth whenever possible, and I still hold speaking it as my first default.

For what it's worth, I agree with them. Yet, I also recognize that speaking truth under every circumstance, regardless of consequence, can, as Bok noted, simply be cruel. And when organizational dynamics come into play, speaking truth can also be potentially risky for the speaker, especially at the point where truth, trust, and loyalty intersect. However, speaking truth to power has always carried a threat to one's reputation and career, and, sadly, I doubt that threat will ever disappear. Yet, in times like these, when truth and falsehood for many are becoming indistinguishable, when society is awash in disinformation and misinformation, and trust appears to be on the wane, I still believe in advocating for truth whenever possible, and I still hold speaking it as my first default.

ABOUT THE AUTHOR

George Lober is a poet and ethicist.

Copyright 2020, George Lober. The US federal government is granted for itself and others acting on its behalf in perpetuity a paid-up, nonexclusive, irrevocable worldwide license in this work to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the US federal government. All other rights are reserved by the copyright owner(s). Foreign copyrights may apply.

NOTES

1. Harry G. Frankfurt, *On Truth* (New York: Knopf Doubleday Publishing Group, 2006), loc. 4, Kindle.
2. Ibid.
3. Ibid.
4. Ibid., loc. 5.
5. Ibid.
6. Ibid., loc. 15.
7. Ibid.
8. Ibid., loc. 16.
9. Sissela Bok, *Lying: Moral Choice in Public and Private Life* (New York: Vintage Books, 2011) loc. 612 and 632, Kindle.
10. Ibid., loc. 708.
11. Ibid., loc. 709.
12. "2020 Edelman Trust Barometer," Edelman, 19 January 2020: <https://www.edelman.com/trustbarometer>
13. Lee Rainie, Scott Keeter, and Andrew Perrin, *Trust and Distrust in America* (Washington, DC: Pew Research Center, 22 July 2019), 46: https://www.people-press.org/wp-content/uploads/sites/4/2019/07/PEW-RESEARCH-CENTER_TRUST-DISTRUST-IN-AMERICA-REPORT_2019-07-22-1.pdf
14. Bok, *Lying*, loc. 763.
15. Ibid., loc. 749.
16. Ibid., loc. 1563.
17. Steven Matthew Leonard, "Hitting the Wall: When Speaking Truth to Power Gets You Nowhere," *ClearanceJobs*, 18 December 2018: <https://news.clearancejobs.com/2018/12/18/hitting-the-wall-when-speaking-truth-to-power-gets-you-nowhere/>
18. Gill Corkindale, "The Price of (Not) Speaking Truth to Power," *Harvard Business Review*, 21 July 2011: <https://hbr.org/2011/07/the-price-of-not-speaking-trut>
19. Ibid.
20. Ibid.
21. Ibid.
22. Rushworth Kidder, *How Good People Make Tough Choices* (New York: HarperCollins, 2009) 6, Kindle.
23. Michel Foucault, "The Meaning and Evolution of the Word 'Parrhesia': Discourse and Truth, Problematicization of Parrhesia," Foucault, last modified 24 October 1983: <https://foucault.info/parrhesia/foucault.DT1.wordParrhesia.en/>

The Game Floor

Cyberspace Operations Training Using *CyberWar: 2025*

By MSG David Tyler Long,
US Naval Postgraduate School

MOST CURRENT CYBER WARGAMES ARE DEVELOPED TO help businesses think through cyber crisis and incident response scenarios. By delving into actions and reactions, these commercial games reveal their roots in traditional military wargames; however, the scenarios they address apply only to the organizations for which they are built, and thus do not have extensive training and education applications outside such organizations. For this reason, a team at the Naval Postgraduate School in Monterey, California, developed *CyberWar: 2025*, an interactive educational wargame that is designed to teach cyberspace operations and can be used on a large scale within government and military organizations.¹ This article describes the design process of *CyberWar: 2025*, focusing in particular on how the game developers incorporated specific cyber concepts and how the game is intended to be used pedagogically.

CyberWar: 2025: Design, Development, and Mechanics

CyberWar: 2025 is a turn-based multiplayer cyber wargame that focuses on the three core cyber-effect categories of defensive cyberspace operations (DCO), offensive cyberspace operations (OCO), and computer network exploitation (CNE).² Using these core categories, players explore the cyber domain, develop and execute a cyber strategy, and react to incoming actions from adversaries within a simulated cyberspace environment. The codebase of *CyberWar: 2025* is written entirely in JavaScript, HTML, CSS, and other open-source libraries to create a sound and interactive game environment suitable for all types of players. The premise of *CyberWar: 2025* was to create a collaborative training environment in which leaders, policymakers, and non-technical personnel partner with those who have experience in cyberspace operations, cybersecurity, or a similar technical field. As a tool to teach cybersecurity, *CyberWar: 2025* is most effective when used in conjunction with a training course. It simulates a realistic cyberspace operational environment and models the effects of current real-world cyber activities in a non-technical and straightforward manner.³

CyberWar: 2025 began as physical gameboards cut from acrylic; after nine months of development, it had evolved into a releasable software project that is cross-platform and lightweight, and requires minimal resources to set up and run (see figure 1). *CyberWar: 2025*'s transformation into a software-based game drastically improved its efficiency and accuracy when compared to the

The complexity of *CyberWar: 2025* lies within the core game mechanics and the dynamic challenges that each player faces from one round to the next.



Figure 1. The early stages of *CyberWar: 2025*. From left to right: two prototype acrylic tabletop boards; the digital beta version in a web browser.

complicated setup of the tabletop version, which required several people to run a single game of 15 rounds within a two-hour window. Hundreds of game modifications and countless hours of code-writing and playtesting were required to produce the final version of *CyberWar: 2025*.

CyberWar: 2025 is an abstract two-dimensional representation of a single cyber network that is divided into six separate sub-domains. At the start of a game, each player controls one of the sub-domains (see figure 2). As the game progresses, players seek to expand into other sub-domains and take control of as much of the board as they can. Think of each sub-domain as a network infrastructure that emanates from the player's base and builds inward to the center of the board. This network infrastructure consists of smaller network points (called Server Nodes in the game) that players have to control in order to gain additional resources known as Action Points. These Action Points can be used by players to conduct cyber-effect research, attack adversaries, and better posture themselves against enemy actions. The overall objective of *CyberWar: 2025* is to dominate the cyber network, either by controlling all available Server Nodes or by denying other players access to these Nodes and thus forcing them off the board and out of the game. Throughout the game session, players have to plan and enact their cyber strategy using the nine cyber-effect attributes available to them, which will be discussed later in this article. Players also have to manage their resources, maintain their cyber network, and defend their base from encroaching adversarial players. The complexity of *CyberWar: 2025* lies within the core game mechanics and the dynamic challenges that each player faces from one round to the next.

Server Nodes (depicted as small hexagons on the gameboard; see figure 2) are the only attack/defend structures

for all actions within the game. From these Server Nodes, players can launch offensive cyberattacks with OCO and CNE effects or defend against incoming attacks with DCO effects; however, the success rate of these effects requires a sound strategy and a bit of luck. When players secure their Server Nodes, they are essentially building up their defenses against other players, while at the same time improving their odds of success in attacking their adversaries.

A fundamental *CyberWar: 2025* mechanism is that of agnostic cyber domain roles. Instead of assigning the players roles that reflect current cyber-threat problem sets, such as state or non-state actors, all players are equal cyber actors on the gameboard.⁴ Players can adjust their role at any time during the game session to suit their cyber strategy, and are free to experiment with their strategy and adapt to the continually changing game environment. With each consecutive round, Server Nodes are captured, lost, and recaptured. Players can have a vast Server Node network one minute and immediately lose their access to other players' domains in the next turn because one critical Server Node was taken by another player or removed from the game board entirely.

Another mechanism within *CyberWar: 2025* is its dependence on the randomization of cyber effects, which is achieved through the integration of a dice roll and the player's attack/defense base value, or Server Node strength. The dice roll yields a randomized value between 1 and 100, simulating a 100-sided die, which is calculated in the software code with each action the players queue in their adjudication lists. Base value and the dice roll combine to provide the player's attack/defend value; if it is higher than the opponent's value, then the action is successful. This randomization also ensures that no two game sessions are identical, even though their outcomes may be similar.

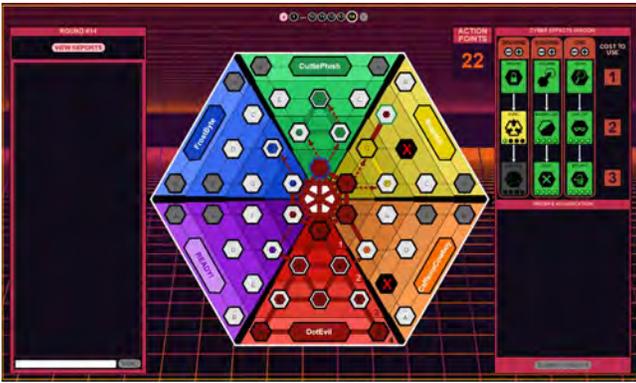


Figure 2. *CyberWar: 2025*, version 1.2

To be successful in the game, players must invest resources in the cyber effects they need to execute their cyber strategy.

Finally, single-player view and “fog of war” make up the most pivotal aspects of the game. *CyberWar: 2025* accommodates an observer view and six individual player views. While the observer view reveals the entire board, the single-player view is limited to the actions of that player, who cannot view another player’s private network without using exploitation effects. This mechanic reflects the real world in that actions in the cyber domain are not readily observable because cyberspace is not tactile. Also, single-player views ensure that opposing players cannot cheat against one another or interfere with another’s planned actions. The “fog of war” effect derives directly from the single-player view: while players see all actions happening within their own domain, actions occurring outside of their domain are hidden. As players venture out on the board and expand their cyber networks by using OCO or CNE cyber effects, the larger operational environment becomes more visible to them.

In addition to the mechanics mentioned above, *CyberWar: 2025* players also need to overcome the challenges of resource management and timing. To be successful in the game, players must invest resources in the cyber effects they need to execute their cyber strategy. Developing and launching each cyber effect has a cost, and that cost is amplified based on the location relationship. This cost accrues when launching cyber effects over domain boundaries between the defender’s and the attacker’s Server Nodes. For example, players executing an effect on Tier 4 Server Nodes outside of their domain add four Action Points to the cost of their cyber effect. The rationale behind this mechanic is to simulate the real-world operational costs

required to initially gain access to a network, such as bypassing a firewall, intrusion detection system, or network gateway.

Nine Cyber Effects

To form and execute a cyber strategy that can dominate adversaries, players must understand the relationships between the nine available cyber effects and how to use each one. The DCO category contains the Secure, Expel, and Analyze cyber effects. The sole purpose of Secure, which is readily available at the beginning of the game, is to build up Server Node defenses to a maximum value of four. Expel, which is used against adversaries who have exploited the defender’s Server Nodes, removes the adversary from those Nodes and prevents him or her from conducting further hostile actions within the defender’s network. Analyze is a modified Scan cyber effect (Scan is a CNE effect and will be discussed later in this section); its only purpose is to identify adversaries who have exploited Server Nodes anywhere across the defending player’s network. An additional effect of Analyze is to identify all the Server Nodes adjacent to the player’s network for potential future cyber actions.

The three OCO cyber effects, Acquire, Manipulate, and Deny, are all overt actions. Acquire takes control of any Server Node, occupied or unoccupied, and is available at the beginning of the game. Once a player acquires a Server Node, the next step is to use Secure to defend it. Only one player can overtly control a single Server Node at a time. Manipulate is a modified form of Acquire, with the only difference being that the attacking player can spoof or mask herself as another player. The significant benefit of Manipulate is to create conflict between two or more rival adversaries or to hide in plain sight on an adversary’s network by using deception and disruption. Deny is the third cyber effect in the OCO category, and it is the “nuclear option.” When successfully launched on a Server Node, Deny permanently removes that Server Node from the playable board, effectively shrinking the operational network. Deny is also the only cyber effect that can be used to remove players from the game by allowing a player to block an adversary’s network access. A player who is deadlocked in this way cannot take any further actions and thus is forcibly removed from the game.

Finally, the CNE category contains the covert cyber effects Scan, Exploit, and Implant. The Scan effect is immediately available and is used to view Server Nodes adjacent to the player’s already acquired Nodes. The only difference between Scan and the DCO effect of Analyze is that Scan

can identify an exploiting adversary one Server Node at a time, but cannot reveal what is happening across the player's entire network. Exploit is the clandestine arm of the OCO Acquire. Exploit has the same mechanics of Acquire; however, Exploit allows multiple players to operate on a single Server Node, whereas Acquire provides one-for-one control. Think of Exploit as a backdoor into a sub-network that other players can access and from which they can maneuver around the network; however, the Server Node itself is still controlled by just one person. Players who have successfully exploited a Node cannot use any of the DCO cyber effects to defend it because they do not actively control it.

Implant is the most expensive CNE cyber effect, and it is the only dual-action effect. As a cyber effect modifier, Implant reduces the Secure strength of a Server Node to its minimum value, rendering that Server Node more vulnerable to attack in that round of play and thus improving the odds for a successful attack. When used in conjunction with one of the attack-based cyber effects (Acquire, Manipulate, Exploit, or Deny), Implant will improve the attack's chances of success. A secondary use of Implant is its ability to freeze an adversary, preventing him from conducting any actions for one round. By using Implant on an adversary's base in this way, the attacking player has a chance to lock out the target player, similar to a ransomware attack on critical infrastructure in the real world. The only differences between Implant in *CyberWar: 2025* and such attacks in reality are that players cannot buy their way out of an Implant attack, and actual ransomware attacks are rarely resolved quickly and easily.

Learning from mistakes through trial and error in a simulated environment is the key to success in wargaming and educational training.

These game mechanics, in combination with the dynamics (e.g., randomization and luck, risks and rewards, competition, and communication) and aesthetics of the game design (e.g., icons, player avatars, colors, and overall visual layout) function together in *CyberWar: 2025* to create an in-depth environment for players that yields a meaningful learning experience and emphasizes replay value. Even though *CyberWar: 2025*'s dynamics and mechanics are abstractions drawn from reality, they are closely related to actual events and current tactics, techniques, and procedures of cyberspace operations and doctrine. The holistic and simplified network view design allows players to focus on the educational value of game play without being

bogged down with technical details and terms, all while having fun and experimenting with new ways to dominate in the cyber environment. Learning from mistakes through trial and error in a simulated environment is the key to success in wargaming and educational training.

Learning Objectives for Cyber Training

Similar to the hundreds of wargames executed throughout history, in which commanders prepared for the battle ahead by using tabletop simulations, *CyberWar: 2025* seeks to prepare warfighters for the battlefield in cyberspace. Although there may never be a single simulation that encapsulates the entirety of cyberspace operations, the game's emphasis on extracting and simplifying historical events and lessons learned in the cyber realm makes *CyberWar: 2025* relevant for current training courses. For example, the nine cyber effects are not specific to any security tool, piece of malware, or virus that is currently identified; instead, they emulate various means to achieve an overall desired result and effect, or reinforce a cyber training and education curriculum. The protocols and standards that currently make up digital networks and systems may not change; however, the methods and tactics used to modify or control those systems or networks may change over time.

This is why *CyberWar: 2025* does not make the intricate low-level details of cyber operations its focal point. Instead, the game deconstructs a few critical aspects of defense/offense operations in cyberspace, reshapes those aspects into game mechanics, and uses them to reinforce key learning objectives and goals for cyber training programs. For its players, *CyberWar: 2025* reinforces a number of learning objectives, such as understanding key terrain and critical infrastructure within the cyber domain, targeting cyber actors, and identifying cyber threats, as well as the

Figure 3. First live tabletop version playtest, 2017



concepts of offensive and defensive operations in cyberspace, to name only a few.⁵

Game Testing and Classroom Application

From the early stages of development, live playtests were essential for the proper evolution of *CyberWar: 2025*. More than 15 playtest sessions, conducted within a span of 18 months, provided the necessary feedback to advance and clarify the game rules, mechanics, and aesthetics, and helped shape *CyberWar: 2025* from a slow and error-prone tabletop game to a lightweight and responsive software beta. These initial playtest sessions consisted of mixed-pairing groups of both technical and non-technical players, with no more than four players per team. This diversity within each team allowed players to learn from each other through interactive problem solving by discussing their overall cyber strategy and next moves amongst themselves.

Before every playtest session, players received a brief bloc of instruction about the rules, the background mechanics, and the relationship between *CyberWar: 2025*'s cyber effects and their real-life counterparts. As each round progressed, players asked questions about their outcomes with the wargame facilitators and discussed potential responses among themselves. After a series of rounds was completed or the time allotted for the game session was up, the game facilitators asked the players to make their final moves and wait for the results. Once the last game-state change was completed, the game director held an open-classroom dialogue by reviewing and analyzing each team's final board view and discussing each of the teams' expectations, strategies, actions, and outcomes. After players had some time to bounce their experiences and "what if" strategies off of each other, they would proceed with a follow-on game session in most cases.

CyberWar: 2025 was designed and developed for collaborative use as a training aid in an in-depth cyber training course or environment.

Of all the playtest sessions, the two most diverse and notable ones were conducted with the staff from the US Air Force Research Lab (AFRL) at Wright-Patterson Air Force Base in February 2019 and with conference attendees at the Military Operations Research Society (MORS) Cyber Wargame and Analytics II workshop in October 2019.⁶ In both game sessions, players were a mix of personnel with both cyber and non-cyber backgrounds and with diverse levels of experience in computer-based wargaming. Most,



Figure 4. Live playtest of the beta version, 2018

if not all, of the players had played some form of tabletop wargame, such as *Pandemic* or *Drive on Metz*.⁷ Just as before, players received a short but detailed bloc of instruction on *CyberWar: 2025*'s game terminology, mechanics, and layout, which allowed everyone to be on the same page and ask questions before game execution. Players then participated in a short five-round game to understand the user interface and become comfortable with the game mechanics. Immediately after this practice run, the game director instructed players to start a new game and begin a live-play session against another team. In the first play session, teams competed against each other for roughly two hours. After a quick post-game review and intermission, the player teams executed a second session for about another two hours. The point of conducting two separate game sessions in one event was to give players the opportunity to rethink their strategies and try different defensive, offensive, or covert tactics.

When a wargaming event was complete, after-action reviews ranged from player teams discussing their confidence, initial pitfalls, and overall understanding of cyber operations to evaluations of the training value behind *CyberWar: 2025*. The only suggestions for improvement from the testers were requests for additional scenarios, modified applications to assist in training private corporations in cyber defense, and a single-player mode to compete against artificial intelligence. The game engine used for the current release of *CyberWar: 2025* does not support these improvements, but an updated game engine is currently in development, as is a commercial version of *CyberWar: 2025*. As of this writing, version one of *CyberWar: 2025* is in continued testing, and is scheduled for release to the public in 2021.

Conclusion

CyberWar: 2025 was designed and developed for collaborative use as a training aid in an in-depth cyber training course or environment. It is not, however, a standalone computer-based training course such as the DoD Cyber Awareness Challenge and, by itself, will not teach anyone how to be a better cyber practitioner. Incorporating *CyberWar: 2025* into a broader instructor-led course allows students to take the information and concepts taught to them in the course and practice those concepts within a simulated and risk-free cyber environment. The iterative and randomized nature of *CyberWar: 2025* gives players the opportunity to learn from past mistakes, and to try new techniques and measures to acquire new outcomes and experiences within the game. Players can then provide feedback from what they learned and engage in an open discussion between one another and with the instructor in the classroom.

Finally, *CyberWar: 2025* is course agnostic, and may be used whether the training program focuses on offensive cyberwarfare or defensive cybersecurity, or anywhere in between. Much like earlier wargames, the mechanics used to create the scenarios are only as effective as the learning objectives supporting them. Instructors will need to determine how they can best weave *CyberWar: 2025* into their programs in order to achieve maximum learning effectiveness.

ABOUT THE AUTHOR

US Army Master Sergeant David “Ty” Long currently serves as a Senior Enlisted Advisor for the US Department 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. David Tyler Long and Christopher M. Mulch, “Interactive Wargaming *CyberWar: 2025*” (master’s capstone, Naval Postgraduate School, 2017): <https://calhoun.nps.edu/handle/10945/56758>
2. Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: Department of Defense, 2018), chap. 2: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150
3. David Tyler Long, “Wargaming and the Education Gap: Why *CyberWar: 2025* Was Created,” *Cyber Defense Review* 5, no. 1 (2020): https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%202012-Long_WEB_1.pdf
4. “Cyber Threat Source Descriptions,” Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, May 2005: <https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions>. An example is an earlier game developed by Global ECCO called CyberStrike, which assigns specific roles and abilities to each player, such as Hacker, Rogue State, Criminal, etc. See <https://globalecco.org/game-lobby>
5. Long and Mulch, “Interactive Wargaming *CyberWar: 2025*,” 22.
6. “IST Hosts Expeditionary Cyber Wargame Event,” Defense Daily, 24 April 2019: <https://www.defensedaily.com/press-releases/ist-hosts-expeditionary-cyber-wargame-event/>; “2019 Cyberspace Wargaming Analytics II Workshop,” Military Operations Research Society, 16 October 2019: <https://www.mors.org/Events/Courses/Past-Courses/2019-Cyberspace-Wargaming-Analytics-II-Workshop>
7. “The World of Pandemic,” Z-Man Games: <https://www.zmangames.com/en/games/pandemic/>; “The Drive on Metz, 2nd ed.,” BoardGameGeek: <https://boardgamegeek.com/boardgame/33030/drive-metz-second-edition>

The Written Word

Rise and Kill First: The Secret History of Israel's Targeted Assassinations by Ronen Bergman

Reviewed by MAJ Daniel Meegan, US Army Special Forces

HOW FAR IS A NATION WILLING TO GO TO PROTECT ITSELF from terrorists? In 1973, in Lillehammer, Norway, Israeli agents gunned down Ahmed Bouchiki in front of his pregnant wife. A Moroccan national who was married to a Norwegian citizen, Bouchiki had become a victim of Israel's global targeted-killing program.¹ Tragically, Bouchiki had been misidentified; he had no connection with terrorism. Worse yet, the Israeli government considered Ahmed Bouchiki's murder to be simply collateral damage in its assassination campaign. Mossad's chief at the time, Zvi Zamir, dismissed the disaster by claiming that "wrong identification of a target is not a failure. It's a mistake." He blamed the victim for behaving "in a manner that seemed suspicious to our people... He may have been dealing in drugs."²

Ronen Bergman provides the details of this operation and dozens of others in his book *Rise and Kill First: The Secret History of Israel's Targeted Assassinations*, one of the most comprehensive books written to date on Israel's targeted-killing campaign. Researched over a span of eight years, *Rise and Kill First* lays out the history of Israel's targeted-killing operations, beginning in the 1930s against the British. The book ends with the last publicly known such operation: the 2010 assassination of Hamas operative Mahmoud al-Mabhouh in Dubai. Israel's targeted-killing program has been the most wide-ranging in the modern world, with over 2,700 known sanctioned operations. Such killings have been documented on every continent but Antarctica, using such methods as shootings, car bomb-ings, mail bombings, poisoned toothpaste, and overdoses of narcotics, to name a few. Both the Israelis and their enemies have engaged in levels of brutality that cannot be overstated. Collateral civilian casualties number in the tens of thousands. *Rise and Kill First* is 784 pages of bloodshed.

As one of Israel's leading investigative reporters, Bergman provides a detailed chronological account of Israel's strategy and reasoning behind the killings.³ He includes 90 pages of notes and bibliography to back up this unofficial history, allowing the reader to further investigate individual events. His research for the book created much controversy inside Israel, particularly within its intelligence community, which was so alarmed by his requests for official documents that



Rise and Kill First: The Secret History of Israel's Targeted Assassinations
By Ronen Bergman

New York: Random House, 2018
784 pages
Hardcover: US \$35.00
Paperback: US \$20.00

it went so far as to have the timeline for declassification of government documents legally extended from 50 to 70 years. This, according to Bergman, was done specifically to thwart his access to information about government-sanctioned killings. Despite these efforts, Bergman was able to find many Israeli commandos and government officials who wanted to have their stories heard. These individuals provided hundreds of documents and sat for thousands of hours of interviews with Bergman, which ultimately enabled him to complete his work.

In addition to its descriptive storytelling and history, *Rise and Kill First* should be important to military leaders for two reasons. First, it provides an 80-year-long case study of targeted kinetic operations against perceived enemies of the Israeli state, offering insight into the methods, tactics, and techniques of the world's most utilized targeted-killing teams. Second, and more important, it shows why explicit policies and oversight by public entities and civilian leadership are paramount to ensuring that military and intelligence operations support national objectives.

Dagan declared that “the state must sometimes perform actions that run counter to democracy.”

Bergman outlines the systematic practice by Israeli military and intelligence leaders of taking matters into their own hands when they felt that policy objectives or civilian oversight would stymie their operations. *Rise and Kill First* shows how these same leaders created many of the same problems they were originally ordered to defeat by prosecuting counterterror operations in whatever way they saw fit. Working off a system that incentivized the killing of terrorists regardless of geographic location, Israeli commandos and assassins embarked on a campaign that spanned the globe. Bergman identifies a structure of extrajudicial killing that was often based less on national goals than on the emotions of military and intelligence commanders. He details numerous occasions when Israel failed to secure even temporary peace, because of personal vendettas by government, military, and intelligence leaders. For example, Meir Dagan, the future head of Mossad, established a secret military unit following the Six-Day War that became known for extrajudicial killings in the Gaza Strip. Most perniciously, the unit had a propensity for letting its captives “escape” and then shooting them because they were escaping. When asked about the unit later on, Dagan declared that “the state must sometimes perform actions that run counter to democracy.”⁴ While Dagan’s unit initially decreased terror attacks

against Israelis, the terror it caused among Palestinians drove them into the arms of the militant Palestine Liberation Organization (PLO).

More disturbing is the reality that these military and intelligence commanders willingly carried out targeted killings in allied and partner nations, often regardless of the consequences to civilians. Israeli special operations units

utilized car bombs, letter bombs, and IEDs against targets in civilian populations in myriad countries, with near impunity. On multiple occasions, Israeli intelligence units tortured captive individuals to death. During one incident in 1984, an Israeli intelligence unit beat two captured terrorists to death with rocks, and then forged evidence to implicate the Israel Defense Forces (IDF). The intent was to make the murders look like the impulsive act of emotional IDF conscripts rather than the work of a professional—and often extralegal—death squad. The unit had an implicit policy of lying to the Israeli government and population in order to maintain the pace of its counterterror operations, in the belief that lying and fabricating evidence furthered its own counterterrorism goals.

Perhaps the most extreme example of the lengths Israel went to in its targeted killing campaign occurred under the leadership of Ariel Sharon. Sharon, according to Bergman, “insisted there was no hope of accommodation with the Palestinians,” while a contemporary of his stated that Sharon could only see Palestinians through the sights of his rifle.⁵ While serving as defense minister, Sharon decided that civilian airplanes from Europe could be shot down if Israeli intelligence thought that Yasir Arafat, the leader of the PLO, was aboard. Despite a raging debate over possible international consequences and the reluctance of the Israeli Air Force (IAF) commander to comply, the IAF conducted intense planning for such an event, even identifying gaps in radar coverage over the Mediterranean Sea that would allow Israeli fighters to shoot down civilian jet liners without being identified. IAF fighters actually flew multiple missions to attack allied civilian aircraft but, fortunately, they were recalled each time because Arafat’s presence on board could not definitively be determined.

This is not to say that many of Israel’s enemies were not brutal in their own right. The use of suicide bombers and rocket attacks against civilians is despicable. However, one



Meir Dagan



can also reasonably assume that Israel is unlikely to improve its relations with its neighbors, and particularly with the Palestinians, when it regularly engages in extrajudicial killings both domestically and abroad. What is worse, these operations have often adopted the same tactics used by the terrorists they are meant to stop, and have even increased recruitment by the groups Israel considers its enemies. As General Yitzhak Pundak, the military governor of the Gaza Strip in the early 1970s, warned, “if we do not give [the Palestinians] a little assistance, a little prosperity, they’ll all turn to the path of terror.”⁶ In a reflection of this irony, Bergman has aptly named one chapter “More Suicide Bombers than Explosive Vests.”

These tales should act as signposts for American military officers and senior officials looking for examples of why objectives, policy, and, most important, civilian oversight must be unequivocal. Military leaders must never forget that they serve their nation and not their personal interests or vendettas. Leaders have a further moral responsibility to ensure that their own conduct and the conduct of their soldiers are of the highest caliber. Counterterrorism operations are a messy business. Leaders must ensure they do not make them messier by adding their own petty objectives to the process.

Bergman's book should cause US political and military leaders to stop and think: Are we doing it right? After 19 years of perpetual kinetic counterterrorism operations by the United States across the globe, have things gotten better or worse? Furthermore, are the policies and objectives coming from above clear

Bergman's book should cause US leaders to stop and think: Are we doing it right?

enough that military leaders on the ground can articulate them? Are these objectives concrete enough that acting outside of them would constitute a clear and gross violation of trust? If this isn't the case, it is logically impossible for military leaders to appropriately and adequately accomplish those objectives. Without clear guidance, military leaders are left to fight as they see fit.

While numerous factors can be blamed for the lack of prolonged peace between Israel and its neighbors, Bergman posits that not least among those factors is Israel's continued targeted killing of civilian and military leaders, without a clear end state. His exhaustive work serves as both a dramatic historical text and a warning of the consequences of encouraging brave men to conduct atrocities, a situation made even worse when they don't fully realize the second and third order effects of their actions. An absolutely worthy read, *Rise and Kill First* should also cause military and civilian leaders to pause and review their own counterterror campaigns to ensure they are not inadvertently perpetuating the conditions that lead to the very terrorism they hope to stop.

ABOUT THE AUTHOR

Major Daniel Meegan is a US Army Special Forces Officer.

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

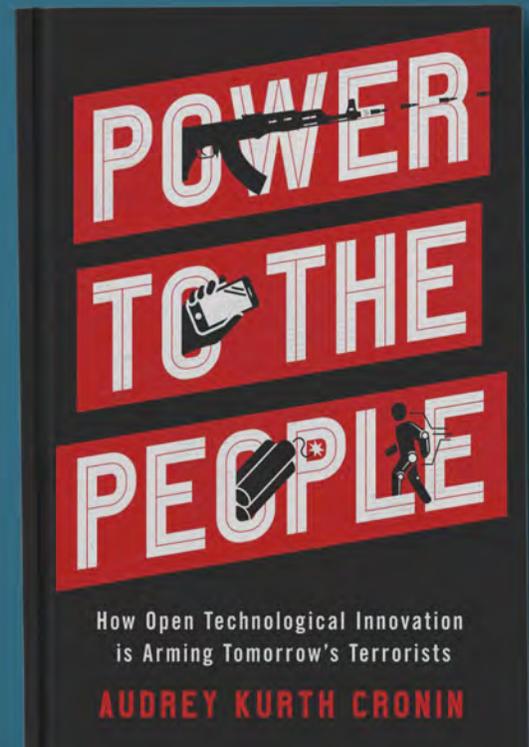
1. While most people may assume that these operations were primarily against Palestinians, the Israeli program is remarkably diverse and far reaching. It has also morphed over time. The initial program was against the British, who occupied Palestine beginning in 1917. After Israel's independence in 1948, it primarily targeted German and Egyptian scientists. The target set expanded over time to include essentially anyone who acted against the Israeli state, but it now focuses largely on Iranians and Palestinians. Victims include British, German, Argentinian, Syrian, Italian, Moroccan, French, Egyptian, Lebanese, and Iranian citizens, to name a few.
2. Ronen Bergman, *Rise and Kill First: The Secret History of Israel's Targeted Assassinations* (New York: Random House, 2018), 182.
3. Ronen Bergman is an award-winning journalist who writes about the intelligence and military communities for Israel's *Yedioth Ahronoth* newspaper and for the *New York Times Magazine*. He holds a PhD in history from Cambridge University and an honors degree from the University of Haifa's Faculty of Law. For further information, see <https://www.penguinrandomhouse.com/authors/129066/ronen-bergman>
4. Bergman, *Rise and Kill First*, 134
5. *Ibid.*, 123.
6. *Ibid.*

The Written Word

Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists

By Audrey Kurth Cronin

Reviewed by MAJ Nate Smith,
US Air Force Special Operations Command



As these malcontents gain power through emerging technologies, the defenses of the law-abiding are increasingly breached.¹

I was intrigued the first time I witnessed the Islamic State in Iraq and Syria (ISIS) using unmanned aerial systems (UAS) to attack Iraqi and Kurdish forces. In early 2018, Syrian rebels carried out the first documented drone swarm attack, using 13 drones to target Russian forces at Khmeimim Air Base and Tartus Naval Facility in Syria.² The ingenuity and creativity displayed by these UAS tactics garnered avid attention from the US Department of Defense, which spent at least \$1.5 billion on counter-UAS (C-UAS) systems in 2018 alone.³ Locating and targeting the individuals responsible for enemy UAS operations also became a significant part of US Special Operations Command's objectives during its campaign against ISIS. For these reasons, I was naturally interested to read Audrey Kurth Cronin's latest book, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*.

Power to the People focuses on how terrorists take advantage of emerging technologies to carry out violence in pursuit of their political objectives, and how open technology is becoming increasingly available to non-state actors, a trend that has the potential to upset global stability. The book considers two technologies that terrorists harnessed for political violence when they first emerged: dynamite and the Kalashnikov rifle (AK-47). Applying the framework of David Rapoport's four waves of terrorism, Cronin makes the case that dynamite and the AK-47 were catalysts for, respectively, the anarchist and anti-colonial waves of terrorism, the first of which began in the late nineteenth century and the second of which continued through the mid-twentieth century.⁴ These disruptive technologies allowed ordinary people to force a shift in power over time from autocrats to citizens.

*Power to the People: How Open
Technological Innovation is Arming
Tomorrow's Terrorists*
By Audrey Kurth Cronin

Washington, DC: Oxford University
Press, 2019
440 pages
Hardcover: US \$28.61

Most military technology, such as nuclear weapons or stealth technology, is developed in a closed, controlled system to which the public does not have access. In recent times, however, we have witnessed an open technological revolution in which increasingly capable computers and associated technologies have quickly become accessible to the public through commercial outlets. The potential of these technologies to upset the balance of power can be seen in the rapid adoption of drones, smartphones, and social media platforms by violent non-state actors.

Lethal empowerment theory helps to explain why some technologies have more potential to be used for political violence than others. According to this theory, disruptive lethal technologies are most likely to diffuse when they are “accessible, cheap, simple to use, transportable, concealable, effective, ‘multi-use,’ not-cutting edge (second or third wave of innovation), off-the-shelf, a cluster of other technology, symbolically resonant, and given to unexpected uses.”⁵ Terrorists rarely, if ever, need to develop new technologies on their own, but simply take what is available and manipulate it for their particular objectives. The theoretical framework of lethal empowerment, coupled with Cronin’s thorough examination of how the use of dynamite and the AK-47 diffused among civilians, provides a suitable lens through which to evaluate the potential for an emerging technology to become a common tool of political violence.

It is very unlikely that Alfred Nobel, the inventor of dynamite, anticipated the ways that his invention could be used in acts of violence when he first patented it in 1867. Dynamite quickly became the first cheap, portable, and easily accessible explosive, which is consistent with Cronin’s lethal empowerment theory. According to Cronin, many scholars overlook the fact that dynamite was the technological innovation that ushered in modern terrorism. The rise of anarchism was fueled by this easily accessible explosive, which, by destabilizing governments, proved to be a catalyst for major state-on-state war. As Cronin notes, “armed with just a few sticks of dynamite, anyone could conduct a terrorist attack of then-unprecedented power.”⁶

Dynamite was the technological innovation that ushered in modern terrorism.

The way dynamite diffused into societies played a crucial role in its popularization among terrorist organizations beginning in the late nineteenth century. Nobel set up

dynamite factories all over the world to meet the insatiable demand for the explosive, a decision that brought the price of dynamite down and made it easily and widely accessible—and also helped make Nobel wealthy. In the United States, a lack of regulatory oversight of the sale and transportation of dynamite further increased its availability to the public. Amazingly enough, it was not until 1970 that the United States enacted a “consistent set of explosive regulations.”⁷ Cronin makes the salient point that once a potentially lethal technology becomes widely diffused, it is often very difficult to reverse the trend or control its spread, “especially if the new technology is commercially produced, has positive uses, and stands to make many people lots of money.”⁸

The AK-47 itself became a high-demand form of currency that could be traded for other commodities.

The AK-47, designed by Soviet Red Army engineer Mikhail Kalashnikov after the Second World War, was a popular technology throughout the second wave of terrorism and into the Marxist/Socialist third wave, and became a symbol for terrorists, insurgents, and freedom fighters from the mid-twentieth century to the present day. The reasons for the AK-47’s success were that it was cheap, easy to use, readily available around the globe, extremely durable, and powerful when compared to similar weapons of the time. Although the AK-47 was originally designed as a tool to help the Red Army fend off invasion, the Soviet Union quickly lost control over the technology because the socialist principles of the USSR did not provide for patents, and the AK-47 itself became a high-demand form of currency that could be traded for other commodities. Because of its capabilities and widespread availability, Cronin argues that the AK-47 “enabled small non-state groups to take on professional armies to a degree that was impossible before the war [World War II].”⁹

Neither Nobel nor Kalashnikov foresaw the large-scale nefarious uses of their technology. Similarly, the creators of the internet, social media, artificial intelligence, and many other emerging technologies failed to anticipate the negative ways in which those technologies are now being used by modern terrorist organizations. These technologies are even more globally diffused and potentially more destabilizing than the AK-47 or dynamite. According to Cronin, “digital online technologies are, in short, atomizing mobilization and shifting the balance of power between states, private actors, and violent groups.”¹⁰ These communication

technologies have increased the range of recruitment for terrorist groups and enhanced the training of those recruits.

Certain emerging technologies are commercially available and can potentially be used to facilitate acts of political violence, such as ISIS's use of drones for surveillance and to drop small explosives on enemy fighters. Cronin examines unmanned aerial vehicles, robots, 3-D printing, and autonomous robots as potentially disruptive technologies in the hands of non-state actors. As technologies develop, the costs and barriers to access typically decrease. The use of drones by ISIS shows that "low-cost, accessible, cheap technologies can have disproportionate effects, especially when combined with surprise, as in a terrorist attack."¹¹ While autonomous weapons are not yet readily available to non-state actors, Cronin reasons that if they do become inexpensive enough and easily accessible, they will most likely become another key destabilizing technology for terrorists and insurgents. There are big profits to be made in artificial intelligence and autonomous technology; therefore, companies have a strong motivation to lower barriers to entry and make these types of technology commercially available.

Cronin concludes by warning that the use of emerging technologies by criminal and violent actors should be anticipated and planned for whenever possible, and that companies such as Facebook and Twitter should be held responsible for the "content they facilitate."¹² She argues that the most effective way to deal with rapid technological innovation is to align "all the participants, including government, industry, and individual citizens, around incentives for developing protections."¹³ If we do not put in place better defensive measures and regulations to deal with the risks, she cautions, the result will be "wars of attrition that democracies cannot win."¹⁴

Power to the People is a compelling analysis of how technology spreads.

Power to the People is a compelling analysis of how technology spreads. By examining how two then-new technologies, dynamite and the AK-47 rifle, spurred periods of terrorism, the book offers insights into how terrorists harness openly available technology in order to wage political violence. In my opinion, however, Cronin's analysis of emerging technologies fails to stand up to the



lethal empowerment theory of technology. For example, while one day 3-D printing, artificial intelligence, and drones may be simpler to operate and more affordable than they are at present, they still will not be comparable to dynamite or the AK-47 in their simplicity and effectiveness. While ISIS's use of drones in Iraq and Syria was a nuisance and received much attention from the US Department of Defense, it in no way shaped the course or outcome of those conflicts. What is more, the threat from armed drones all but disappeared once their operators were removed. The most accurate predictions for the use of emerging technology focus on those that affect mobilization and recruitment: communication technologies. Dynamite would not have been as effective in helping terrorists achieve their political goals without propaganda delivered through sensationalist newspapers, and the AK-47 would not continue to be as effective as it is if not for the advent of the 24-hour live news cycle. While there is potential in the future for some of the emerging technologies to be used for negative purposes, I believe that it is the rapid growth and diffusion of information and communication technology that will prove to be the most destabilizing and powerful tool for extremists.

ABOUT THE AUTHOR

Major Nate M. Smith is a career pilot with the US Air Force Special Operations Command.

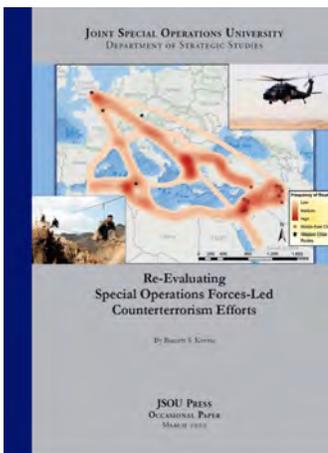
This is a work of the US federal government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

NOTES

1. Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (New York: Oxford University Press, 2019), 1.
2. "Syria: Drone Swarm Attacks Russian Military Bases," TRIPwire, 12 January 2018: <https://tripwire.dhs.gov/news/209478>
3. "Special Report: US Department of Defense Spending on Counter-UAS Reaches USD 1.5 Billion in 2018," Unmanned Airspace, 4 November 2018: <https://www.unmannedairspace.info/counter-uas-systems-and-policies/special-report-us-department-defense-spending-counter-uas-reaches-usd-1-5-billion-2018/>
4. Rapoport describes four waves (note that all date ranges are approximate): anarchism (1880s to 1920s), anti-colonialism (1920s to 1960s), new left (1960s to 1990s), and religious extremism (1979 to the present). For more on this theory, see David C. Rapoport, "The Four Waves of Modern Terror: International Dimensions and Consequences," ResearchGate, January 2013: https://www.researchgate.net/publication/286896869_The_four_waves_of_modern_terror_International_dimensions_and_consequences
5. Cronin, *Power to the People*, 13.
6. Ibid., 74.
7. Ibid., 123.
8. Ibid.
9. Ibid., 162.
10. Ibid., 180.
11. Ibid., 209.
12. Ibid., 260.
13. Ibid., 264.
14. Ibid., 267.

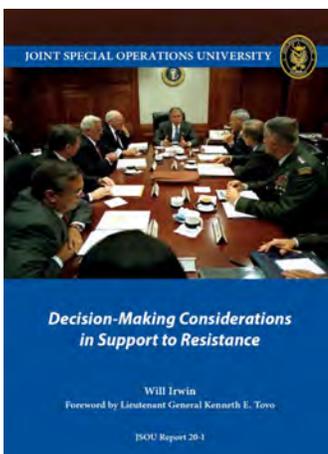
JSOU Publications

These recent Joint Special Operations University (JSOU) Press publications are available electronically on the USSOCOM Research Library website in the JSOU Press Publications 2019 and 2020 sections: <https://jsou.libguides.com/jsoupublications>



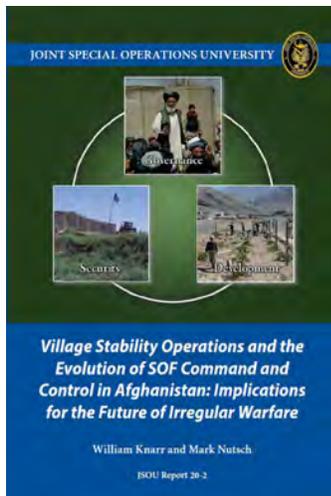
Re-Evaluating Special Operations Forces-Led Counterterrorism Efforts by Barnett S. Koven

Dr. Koven, in this occasional paper, posits that kinetic counterterrorism (CT) actions undertaken by the state to kill, capture, or otherwise disrupt terrorist groups are ineffective in isolation. While kinetic actions may succeed in disrupting a specific plot or other activities in the immediate term, they have little long-term effect on the ability of terrorist groups to operate. This study, backed by data from Colombian CT efforts over several years, demonstrates that government CT activities leading to the capture, killing, or demobilization of terrorists are correlated with an increase in terrorist attacks following a government's actions. Moreover, this study reasons that government actions also serve to diffuse terrorist attacks into surrounding municipalities. Although kinetic CT actions may appear effective insofar as terrorist violence in the immediate vicinity of the CT actions decreases, if terrorism is displaced to other areas, this is not truly indicative of success. Dr. Koven's research suggests that successful CT approaches will require carefully sequenced kinetic and non-kinetic approaches.



Decision-Making Considerations in Support to Resistance by Will Irwin with Foreword by Lieutenant General Kenneth E. Tovo

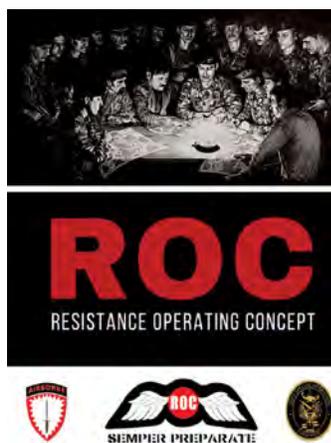
The intent of this monograph is to reveal to Special Operations Forces (SOF) leaders and planners the variety of considerations facing decision makers, the approaches used in strategic- and operational-level decision making, and how they can better inform and influence that process with regard to special warfare. This monograph is a companion volume to two earlier works: "Support to Resistance: Strategic Purpose and Effectiveness," and "How Civil Resistance Works (And Why It Matters To SOF)." This third volume describes some of the factors that decision makers have faced when considering support to resistance (STR) as a foreign policy option. This monograph sheds some light on how national security officials in the past have arrived at certain conclusions and why, in some cases, presidents have directed actions that were especially risky or controversial.



Village Stability Operations and the Evolution of SOF Command and Control in Afghanistan: Implications for the Future of Irregular Warfare

by William Knarr and Mark Nutsch

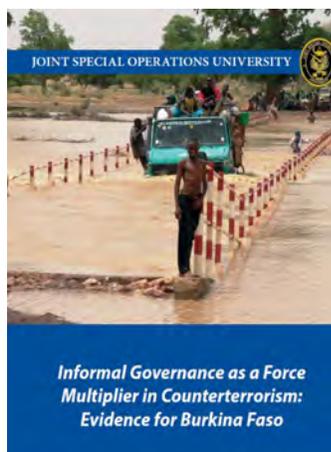
In this monograph, Bill Knarr and Mark Nutsch recount how Special Operations Forces (SOF) command and control evolved along with all of the Village Stability Operations (VSO) dimensions, which culminated in the creation of the Special Operations Joint Task Force. The 2018 National Defense Strategy called for expanding the competition space below the level of armed conflict. VSO provides a timely and relevant example of how SOF can contribute to this vision. Just like terrorism, great power competition will play out in countries with weak sociopolitical systems. The inherently political character and joint, interagency, international/multinational, and corporate nature of VSO can be replicated in many parts of the world for sustainable strategic effect. This monograph develops the concepts for SOF on how to contribute more effectively and efficiently to the counterterrorism fight, but readers would do well to think about VSO principles and command and control in the context of great power competition.



Resistance Operating Concept (ROC)

by Otto C. Fiala, with a Foreword by Major General Kirk Smith and Brigadier General Anders Löfberg

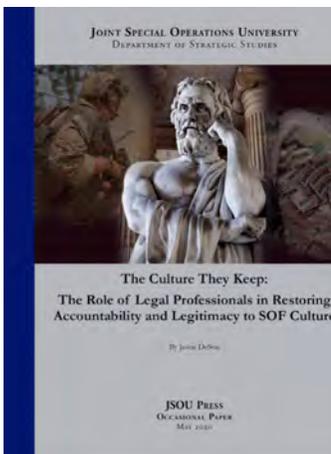
The primary focus of the Resistance Operating Concept (ROC) is to develop a nationally authorized, organized resistance capability prior to an invasion and full or partial occupation that result in a loss of territory and sovereignty. Resistance, as a form of warfare, can be conceived as part of a layered, in-depth national defense. Toward this end, the ROC first seeks to delineate the concept of national resilience in a pre-crisis environment. Second, the ROC seeks to develop resistance requirements, and support planning and operations in the event that an adversary compromises or violates the sovereignty and independence of an allied or partner nation. The ROC attempts to demonstrate both the significance of national resilience and the criticality of maintaining legitimacy during the conduct of resistance operations during the struggle to restore and resume national sovereignty. This publication will serve as a cornerstone of knowledge for strategists, policymakers, researchers, academics, and practitioners involved in furthering resistance capabilities.



Informal Governance as a Force Multiplier in Counterterrorism: Evidence for Burkina Faso

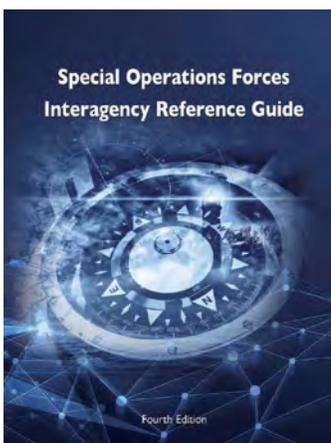
by Margaret H. Ariotti and Kevin S. Fridy

Dr. Kevin Fridy and Dr. Molly Ariotti assert that a CT effect in Burkina Faso can be more fruitfully generated by incorporating the range of Burkinabé informal governance providers into joint, interagency, and partner operational concepts. Although joint doctrine correctly notes the host nation (HN) government must invite U.S. Special Operations Forces into the country, it errs in assuming that only the HN provides the population with governance. By differentiating between the concepts of government and governance, Fridy and Ariotti demonstrate how local political legitimacy can be enhanced—and the allure of violent extremist organizations diminished—by enhancing indigenous, informal governance structures. Although written from the perspective of CT, readers are encouraged to imagine how SOF could apply the insights in the context of great power competition as well.



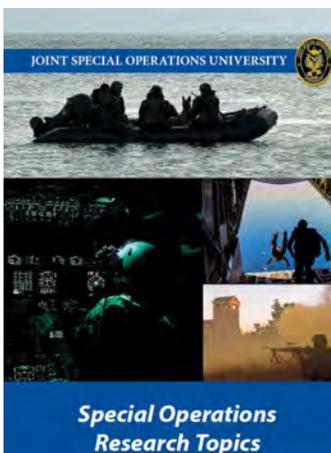
The Culture They Keep: The Role of Legal Professionals in Restoring Accountability and Legitimacy to SOF Culture by Jason DeSon

In this award winning paper, Lieutenant Colonel Jason DeSon looks at Special Operations Forces (SOF) culture and how the legal professionals within the USSOCOM can help restore an ordered value system. He asks the question, “If a disordered value system is truly the source of the current ethical and cultural shortcomings of SOF—where individual and team considerations come before ethical standards—then what role, if any, do the legal professionals of the Judge Advocate General’s Corps supporting SOF have in enabling the commander to overcome those shortcomings and promote a culture of adherence to those high standards of ethical and professional conduct?” Lt. Col. DeSon proposes a four-step process to help clarify the SOF culture problems and develop solutions.



Special Operations Forces Interagency Reference Guide, Fourth Edition edited by Charles Ricks

Mr. Charles Ricks, a JSOU Senior Fellow, first compiled this guide over a decade ago and continues to provide updates and revisions so that it remains a valuable reference work for JSOU students, Special Operations Forces (SOF) staff officers, and partners within the interagency (IA) enterprise. This is now the fourth edition of this publication. This new edition recognizes the changing nature of the international security environment and the adaptive and evolutionary nature of the IA process. While counterterrorism and combating terrorism remain essential SOF activities, the IA concepts, principles, and processes discussed here apply similarly to the involvement of SOF across the entire competition continuum and to all SOF core activities. As noted by the fifth SOF Truth, “Most special operations require non-SOF support.” That reality continues to form the basis for this guide as it addresses SOF IA engagement across the entire international competition continuum.



Special Operations Research Topics 2020 (Revised Edition for Academic Year 2021)

The JSOU Special Operations Research Topics 2020 publication, newly revised for academic year 2021 with 18 new topics, highlights a wide range of research topics collaboratively developed and prioritized by experts from across the Special Operations Forces (SOF) community. As with the previous versions of this publication, this list is tailored to address special operations priorities. The topics in these pages are intended to guide research projects for professional military education (PME) students, JSOU faculty, fellows and students, and others writing about special operations during this academic year. This research will provide a better understanding of the complex issues and opportunities affecting the strategic and operational planning needs of SOF.

Image Credits

Page 1: Photo by IRANIAN SUPREME LEADER PRESS OFFICE / HANDOUT/Anadolu Agency via Getty Images

Page 5: JOHN THYS/AFP via Getty Images

Page 6: ROBIN VAN LONKHUIJSEN / AFP via Getty Images

Page 7: Defense / CC0

Page 8: Today Testing (For derivative) / CC BY-SA (<https://creativecommons.org/licenses/by-sa/4.0>) Geralt / CC0

Page 10: Dr. Hubertus Knabe / CC BY-SA (<https://creativecommons.org/licenses/by-sa/4.0>)

Page 12: Public domain

Page 13: Anthony Crider / CC BY (<https://creativecommons.org/licenses/by/2.0>) Page 14:

Page 15: Diliff / CC BY-SA (<http://creativecommons.org/licenses/by-sa/3.0/>)

Page 16: Bundesarchiv, Bild 102-13378 / CC-BY-SA 3.0 / CC BY-SA 3.0 DE (<https://creativecommons.org/licenses/by-sa/3.0/de/deed.en>)

Page 17: Unknown author / Public domain

Page 18: Saeid Zareian / picture alliance via Getty Images)

Page 20: Pete Marovich / WHITE HOUSE POOL (ISP POOL IMAGES)/Corbis/VCG via Getty Images)

Page 22: Jabin Botsford / The Washington Post via Getty Images)

Page 24: English: R. D. Ward / Public domain

Page 26: Copyright World Economic Forum (www.weforum.org), swiss-image.ch/Photo by Monika Flueckiger / CC BY-SA (<https://creativecommons.org/licenses/by-sa/2.0>)

Page 28: François Lemoyne / Public domain

Page 29: Princeton University Press

Page 29: Amazon

Page 30: Clinton White House / Public domain

Page 30: Amazon

Page 40: Amazon

Page 41: IDF Spokesperson's Unit / CC BY-SA 3.0

Page 42: Public domain

Page 44: Amazon

Page 46: Mussi Katz / CC0

Terms of Copyright

Copyright © 2020. 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 counterterrorism 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 “Submit to CTX” link, click on “CTX Journal,” and then click on the “Submissions” link.

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 (no longer than 15 minutes)
- **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 re-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.

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:

- 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 consent from anyone whose pictures, videos, or statements you include in your work.
- You must agree to our Terms of Copyright.
- 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).

CTX is online at globalecco.org

