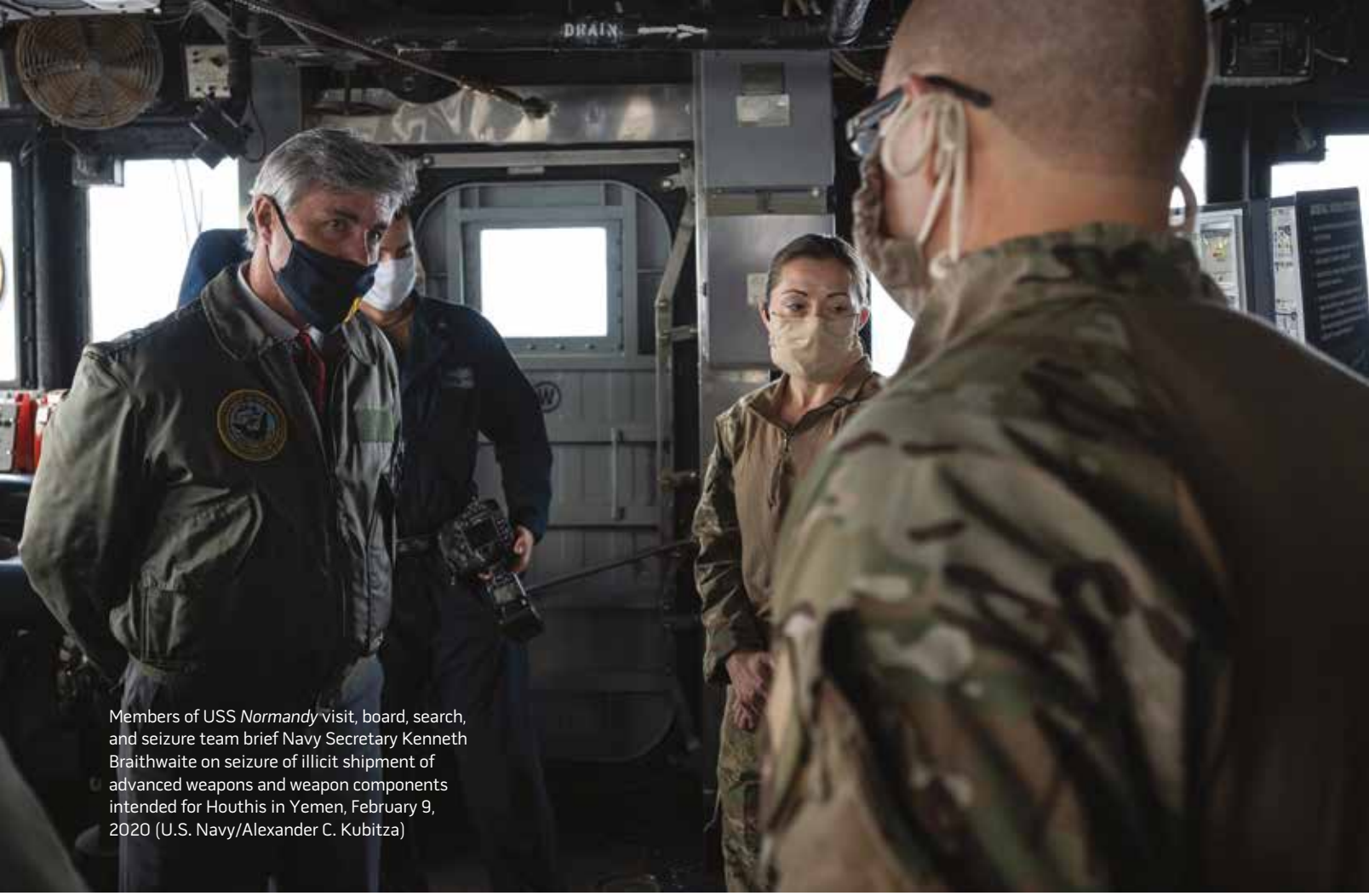


Members of USS *Normandy* visit, board, search, and seizure team brief Navy Secretary Kenneth Braithwaite on seizure of illicit shipment of advanced weapons and weapon components intended for Houthis in Yemen, February 9, 2020 (U.S. Navy/Alexander C. Kubitza)

The Strategic Potential of Collected Exploitable Material

By Michael R. Fenzel with Leslie Slootmaker and R. Kim Cragin

In November of 2007, I was commanding an infantry battalion in the Eastern Paktika Province of Afghanistan. One of our convoys was hit by an improvised explosive device (IED) on a routine mission in the border district of Bermel, just a few short miles from Pakistan. A brilliant young troop commander (Captain David Boris, USA, age 30) and his dependable and tough driver (Sergeant Adrian Hike, USA, age 26) were killed in the explosion.[1]

A few questions came to mind as I struggled with the loss. Who had built and placed the IED? How could I exact justice? What actions could I take to prevent a recurrence? This is the timeless dilemma of every commander in combat. It is personal. It does not matter that the attack occurred in a time of war. It is of no consolation to understand "the enemy has a vote." Thirteen years later, as I reflect back, it was this searing event and my talented staff's response that taught me the value of collected exploitable material (CEM).[2]

After the Bermel attack, an explosive ordnance disposal (EOD) team conducted a postblast analysis of the site and found what would prove to be critical

Major General Michael R. Fenzel, USA, is Vice Director for Strategy, Plans, and Policy (J5). Commander Leslie Slootmaker, USN, is assigned to the Directorate for Strategy, Plans, and Policy (J5), Global Integration, at the Pentagon. Dr. R. Kim Cragin is a Senior Research Fellow at the Center for Strategic Research, Institute for National Strategic Studies, at National Defense University.

Afghan National Army soldiers, combined with assets from 45th Infantry Brigade, conduct cordon and search in village thought to be home to IED makers and Taliban fighters, August 21, 2011, in Alingar District, Laghman Province (DOD/Ryan Crane)

CEM. Specifically, the EOD team collected a pressure plate with metal soup can lids and wire taped together at one end. The team also recovered fragments of a battery pack wrapped in goat hair. Biometrics (fingerprints) were lifted from the tape. In addition to the EOD team, I had a retired Federal Bureau of Investigation (FBI) agent serving on my staff. He informed me that the same fingerprints had been discovered at the site of four other IED attacks. He explained how the distinctive configuration of these IEDs was the "signature" of a single bombmaker. If we could locate him, then we would have the person responsible for killing Captain Boris and Sergeant Hike.

Five months later, a local goat herder told us that bombs were being made in a *qalat* (a fortified place) in Bermel. A combined Afghan army and coalition team searched the dwelling and found the same distinctive bombmaking materials. The bombmaker and his fellow insurgents were detained, taken to prison in Kabul, and, based on evidence derived from the CEM, convicted of terrorism charges under Afghan law. We subsequently saw an immediate and dramatic reduction of IED activity in Bermel.

This story is not uncommon. The Armed Forces often acquire large quantities of CEM in the midst of operations. Even now, we hold over 300 terabytes of CEM gathered from across the globe.[3] It has become common practice for ground force commanders to use CEM as they "find, fix, finish" violent extremist organizations (VEOs) on the battlefield.[4] Less frequently, and outside of conflict zones, law enforcement authorities have used CEM in criminal proceedings against a wide variety of illicit actors. CEM has proved useful in securing longer prison sentences for convicted terrorists and persuading countries to extradite terrorists to the United States. Yet CEM has its challenges. Transfers or "warm handoffs" between the U.S. military, law enforcement, and other government agencies have been inefficient and cumbersome.[5] The Armed Forces also have struggled to get these materials to our allies and partners in a usable format and timely manner.[6]

To address these challenges, Secretary of Defense Mark Esper in January released new guidance on CEM in a memorandum titled "Classification of Materials Captured, Collected, or Handled by the Department of Defense." The memo directs that all new CEM be unclassified unless sensitive sources, methods, or activities were used to acquire it.[7] The document articulated the following logic:

Sharing of CEM with foreign partners is often necessary to effectively prosecute persons who pose a clear and present danger to the safety and security of the United States and our foreign partners in civilian courts of law. . . . Unclassified CEM is releasable to the public and partner nations to support the U.S. mission objectives

and partner nation security and law enforcement purposes, to include criminal prosecutions.[8]

This new guidance lays the foundation for CEM to be used well beyond the battlefield. It allows for easier transfer of CEM from the military to other U.S. Government agencies, as well as our allies and partner nations. Yet substantially more work needs to be done. This article argues that, to realize its full potential, CEM also should be leveraged as part of strategic competition.[9]

To do this, the article first examines recent efforts by the Armed Forces to acquire CEM during operations against VEOs and transfer it to law enforcement authorities in the United States, our allies, and partner nations. The article explores three different types of CEM: al Qaeda's internal memos and correspondence gathered in conjunction with the Abbottabad raid, IED components collected as part of "Omar's Cache" in Baghdad, and, more recently, so-called Islamic State (IS) registration forms captured during Operation *Inherent Resolve*. Second, the article discusses how the lessons learned from these counter-VEO operations apply to strategic competition. In doing so, the article provides some concrete, albeit limited, examples of how the Armed Forces have used CEM to counter Iran's malign activities and how a similar approach could be taken with Russia and China. The article concludes with an appeal to the joint force to think more creatively about the application of CEM, in combination with other instruments of National power, to confront rogue states and revisionist powers.

Lessons Learned from the VEO Fight

In May 2011, Army aviators and Navy SEALs executed a raid against then–al Qaeda leader Osama bin Laden's compound in Abbottabad, Pakistan. The SEALs killed bin Laden and captured over 470,000 electronic files from his compound.[10] These documents represent the most well-known recovery of CEM by the Armed Forces in modern history.

But that is not the end of the story. One of the Abbottabad documents linked Saleh al-Somali, al Qaeda's then–head of external operations, to an individual named Abid Naseer. Naseer was already in a British prison at the time of the raid.[11] He was arrested in April 2009, along with three other terrorists for plotting attacks on behalf of al Qaeda in New York City, Manchester, and Copenhagen.[12] British authorities extradited Naseer to the United States, and U.S. prosecutors were able to use documents from the Abbottabad raid to secure a 40-year prison sentence for him.[13] This example illustrates how CEM can assist prosecutors in their efforts to connect individual terrorists to foreign VEOs and their global terrorist networks. It also underscores the critical need for the Armed Forces to appropriately classify (certainly not misclassify) these types of materials at the point of collection in order to preserve the ability of prosecutors to use CEM in civilian criminal courts.

This same logic—that is, making CEM available for criminal proceedings—recently enabled the extradition of a bombmaker from Turkey to the United States, as well as his successful prosecution in Arizona. Syrian terrorist Ahmad Ibrahim Al-Ahmad built IEDs for Iraqi insurgent groups to use against the Armed Forces deployed to Iraq during Operation *Iraqi Freedom*. Some of his devices were discovered during an August 2006 raid on an IED factory on 50 Omar Street in Baghdad.[14] We gathered these devices, colloquially referred to as "Omar's Cache," and, in partnership with the FBI, collected biometrics in anticipation of using this CEM in the future. This effort eventually proved its value. Unbeknownst to the United States, Al-Ahmad left Iraq in July 2010 and relocated to China. He continued to build and ship IED components to Iraqi insurgents while living there. But in May 2011, Al-Ahmad attempted to return to Iraq by way of Istanbul, and Turkish authorities arrested him. Three years later (2014), the U.S. Government persuaded Turkey to extradite Al-Ahmad to the United States for prosecution based on the CEM found in Omar's Cache and an International Criminal Police Organization (INTERPOL) Red Notice.[15] By the time Al-Ahmad was extradited, he had shifted his allegiance from the 1920 Revolution Brigade to the Islamic State.[16]

Beyond prosecutions, the Armed Forces have provided CEM to allies and partner nations to assist with efforts to identify and arrest terrorist plotters before they can execute attacks in the West. As an example, in October 2015, the Armed Forces captured a cache of documents from IS and shared them with Danish authorities.[17] The cache contained registration forms from foreign terrorist fighters who had left their homes in Western Europe and traveled to the Middle East to join IS.[18] As it happens, IS is a highly bureaucratic VEO that uses payrolls, guest house registries, weapons inventories, leave requests, and registration forms. On the captured forms, IS required applicants to provide recruiters with their name, nationality, residence, skill set, and education.[19] The forms also outlined the duties performed by IS members.[20] In April 2016, using information from these forms, Danish authorities identified and arrested five individuals who had fought for IS in Syria and returned home to plot attacks in Europe.[21] The actions of Danish authorities in this case demonstrate potential for CEM to prevent terrorist attacks in the West. To do so, however, the Department of Defense (DOD) must take measures to ensure CEM is not only properly classified and catalogued but also made quickly and readily available to allies and partners.

At this time, the joint force, our allies, and partners have all learned the value of collecting, storing, and cataloguing CEM with the expectation of eventually employing them against VEOs.[22] The idea of using CEM in criminal proceedings is not new. The International Criminal Tribunal for the Former Yugoslavia heard evidence gathered by military police in coordination with the Office of Prosecutor in Srebrenica (1995) and Kosovo (1999). In fact, the evidence accounted for an estimated 65 percent of the total evidence used by the Office of the Prosecutor.[23]

Yet some allies and partner nations continue to struggle in their efforts to introduce CEM into civilian criminal court proceedings. Most of the concern centers on the admissibility of materials captured, collected, or stored by the military from the battlefield.[24]

To alleviate these concerns, the United Nations (UN) in January of this year issued guidelines for the use of battlefield evidence in the criminal prosecution of foreign terrorist fighters.[25] The purpose of these guidelines is to assist UN members in updating and modifying legal frameworks to allow for use of CEM in criminal proceedings. Just as Secretary Esper's memo urges, UN guidelines emphasize the importance for all countries to declassify battlefield evidence and make it readily available for criminal proceedings. The guidelines state:

To ensure the most effective possible use of information in criminal proceedings, States are encouraged to refrain from over-classifying such information. They are also encouraged to develop simplified procedures for the declassification of such materials where they are likely to be used in such proceedings.[26]

The joint force is at the forefront of global efforts to collect, properly classify, declassify, and catalogue CEM so that it can be used as evidence in criminal proceedings against VEOs.[27] Due to these efforts, the FBI has used CEM to identify and arrest terrorists who pose a threat to the U.S. homeland. It is also working to share CEM with its counterparts globally.[28] U.S. attorneys have prosecuted individuals successfully with CEM in the United States, and the Department of Justice has shared this experience with prosecutors worldwide.[29] Yet more work remains to be done. The joint force needs to continue to apply the aforementioned lessons learned from the successful application of CEM to the ongoing fight against violent extremism. This means investing the resources, time, and effort to break down barriers to collection, classification, and sharing of CEM, both domestically and internationally. But it is also the right time to take the lessons learned from the use of CEM to confront VEOs and apply them to strategic competition.

Applications for Strategic Competition

While the joint force's use of CEM in the fight against VEOs is well documented, CEM also holds unlimited potential for strategic competition. It simply requires creativity in the application. This viewpoint aligns with the 2018 National Defense Strategy, which describes both the central challenge to U.S. national security and the required response as follows:

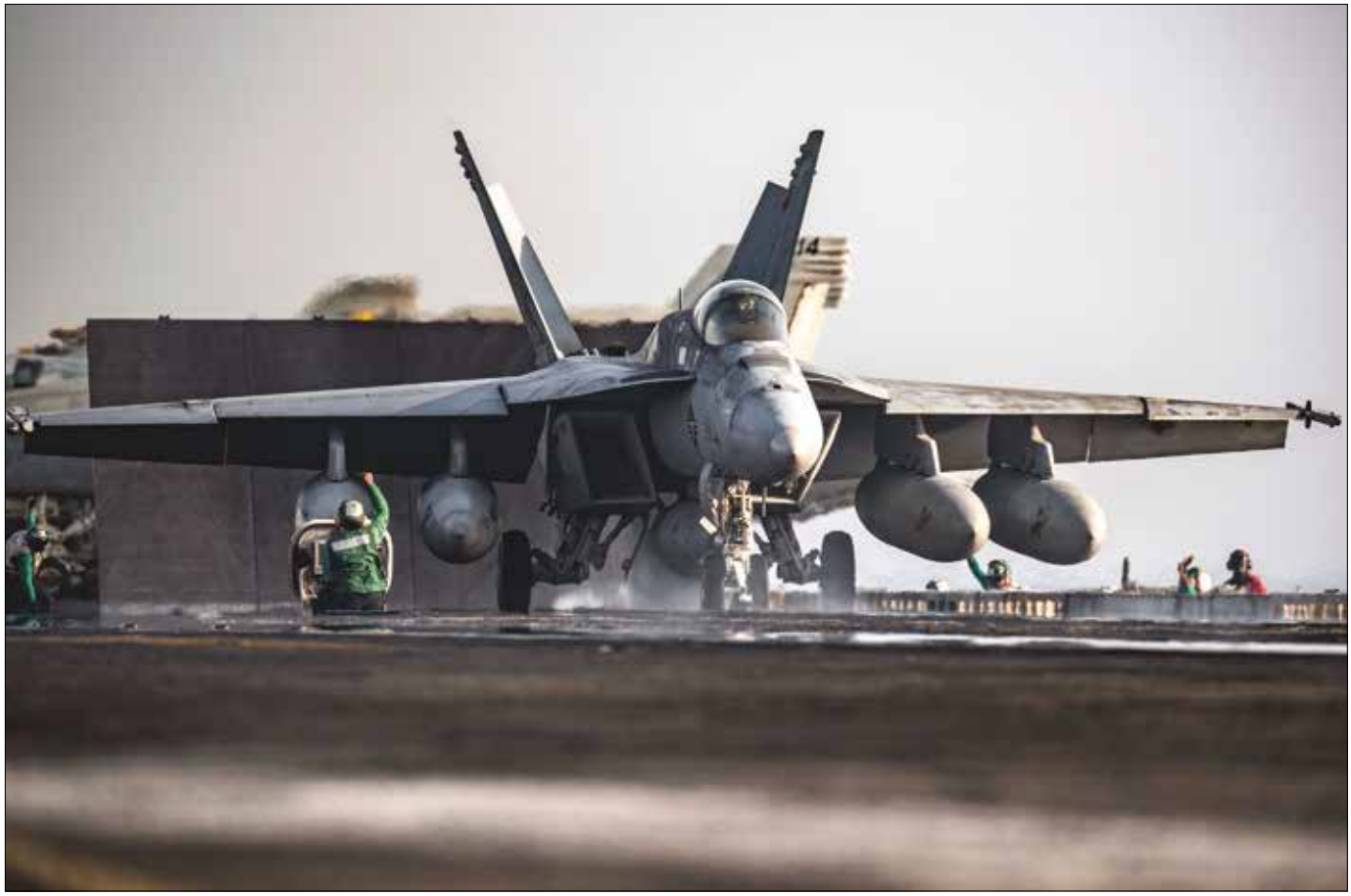
The central challenge to U.S. prosperity and security is the reemergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.

A long-term strategic competition requires the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military.[30]

When the National Defense Strategy calls on the joint force to be more competitive by looking at its own capabilities relative to these revisionist powers over the long term, it is best understood as part of a wider effort to push back or resist this encroaching authoritarian model that is inimical to U.S. interests. This wider effort includes not only military capabilities and strength but also diplomacy, information, economics, finance, intelligence, and law enforcement. Both the National Defense Strategy and the National Military Strategy emphasize competition *below the level of armed conflict*. They also describe strategic competition as a collective effort with the United States, its allies, and partner nations.[31]

Given this understanding of strategic competition, CEM seems well positioned as a means to foil any country's use of private military companies (PMCs), paramilitaries, and proxy forces. Some of this is already being done. For example, looking at the U.S. Central Command area of responsibility, the United States recently used CEM recovered by the Armed Forces to highlight Iran's illegal support to Houthi insurgents in Yemen. On November 25, 2019, the USS *Forrest Sherman* legally boarded an unregistered *dhow* (small sailing vessel) in international waters and seized CEM containing unmanned aerial system components, antitank-guided missiles, "near-fully assembled" Iranian surface-to-air missiles, 13,000 blasting caps, and other missile components.[32] A few months later (February 9, 2020), the USS *Normandy* seized a similar cache.[33] In both interdictions, close coordination occurred among DOD, law enforcement, partner nations, and UN weapons inspectors. Indeed, allowing UN inspectors access to this CEM in a timely manner proved critical; the inspectors confirmed and announced to the international community that the weapons were produced by Iran.[34] Secretary of State Mike Pompeo, in turn, has used this CEM in his diplomatic engagements to urge the UN Security Council to extend the arms embargo against Iran.[35]

If CEM can be used effectively in this way against rogue states, such as Iran, it also has applications for strategic competition with revisionist powers. Russia, and its use of PMCs, represents an obvious example. It is well known that the Wagner Group is a Russian PMC led by former Glavnoye Razvedyvatelnoye Upravlenie officer Dmitry Utkin.[36] In June 2017, the Department of Treasury sanctioned Utkin and the Wagner Group for their involvement in Russia's illegal annexation of Crimea.[37] Its fighters directly confronted Special Forces deployed to Syria in February 2018.[38] The Wagner Group also sent weapons along with 1,200 fighters to Libyan General Khalifa Haftar's forces in violation of UN sanctions.[39] In fact, UN sanction monitors recently released details on 122 individuals linked to the Wagner Group who were in Libya to either transfer weapons, provide training to Haftar's forces, or fight.[40]



F/A-18E Super Hornet, assigned to Gunslingers of Strike Fighter Squadron 105, launches from flight deck of USS *Dwight D. Eisenhower,* Arabian Gulf, August 8, 2016, in support of Operation *Inherent Resolve* (U.S. Navy/J. Alexander Delgado)

If the United States, its allies, or partner nations obtained CEM on these individuals, they could substantiate INTERPOL notices and warrants for the paramilitaries' arrests or requests for extradition. Alternatively, CEM used in diplomatic engagements could encourage our allies and partners to enact travel restrictions on the Wagner Group or other relevant Russian PMCs. If successful, these efforts would undermine Russia's ability to send PMCs abroad to bolster authoritarian regimes or otherwise use them as an instrument of foreign policy.

China, and its use of front companies, provides another opportunity to use CEM as part of strategic competition. CEM could be used to defend against Chinese front companies attempting to steal U.S. intellectual property, including military technology. In May 2017, the FBI arrested Shan Shi, a U.S. citizen, and charged him with attempting to steal trade secrets for a Chinese company, CBM-Future New Material Science and Technology Co., Ltd. (CBMF), and by extension the Chinese government.[41] China does not have the indigenous capability to produce syntactic foam, which is a dual-use technology with applications for deep water oil exploration, as well as Navy submarines and warships. Shan Shi created a front company in Houston and partnered with CBMF to steal this intellectual property.[42] CBMF paid Shan Shi $3.1 million between 2014 and 2017.[43] Using this money, Shan Shi hired employees away from a Houston-based subsidiary of the Swedish company that manufactures syntactic foam, Trelleborg. Shan Shi's new employees obtained spreadsheets from their former colleagues at Trelleborg with details on how to produce syntactic foam and passed this information along to Shan Shi, who then emailed it to CBMF in China.[44] These spreadsheets, emails, and other communications represent just another type of CEM.

Through reciprocal sharing, DOD could use such CEM-derived information to better protect and secure our vital assets and intellectual equities. This information is also an ideal tool for diplomatic engagements, such as highlighting China's efforts to expand its capabilities through the illegal use of front companies or persuading allies and partner nations to enact measures to halt illegal behavior.

These examples illustrate the utility of CEM as an instrument of national power.[45] It has diplomatic, informational, economic, intelligence, law enforcement, and military applications—all of which are named in the National Defense Strategy as elements integral to strategic competition. In order to reach its full potential, however, the declassification and distribution of CEM should be a collective endeavor, including the U.S. Government, allies, and partner nations. Other militaries and law enforcement organizations would need to collect,

properly classify, and share these materials with the United States in a transparent manner, allowing for fulsome exploitation in our counterintelligence efforts, criminal proceedings, and diplomatic engagements.

Final Thoughts

Collected exploitable material provides golden opportunities for collaboration among the joint force, interagency community, allies, and partner nations in the fight against violent extremism. Equally important, the joint force now has a growing body of lessons on the effective utilization of CEM that it can apply in the ongoing competition with revisionist powers and rogue states. Strategic competition requires us to think innovatively, work collaboratively, and utilize every instrument of national power at our disposal. As we begin to think critically through the application of CEM across multidomain operations—domains less developed or yet to be discovered—we must understand that CEM, if applied in this context, provides a myriad of opportunities. Let's not miss them. **JFQ**

Notes

[1] "Honor the Fallen," *Military Times*, available at <https://thefallen.militarytimes.com/army-capt-david-a-boris/3190019>.

[2] Collected exploitable material is all material and/or materiel in the possession of the Department of Defense, regardless of its classification or how it was obtained, that could be exploited in support of DOD and National interests. Examples range from fingerprints and other biometrics to bomb-making materials to internal memos produced and distributed by terrorist leaders. See Mark Esper, "Classification of Materials Captured, Collected, or Handled by the Department of Defense," memorandum, DOD, January 9, 2020; and *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings* (Washington, DC: International Institute for Justice and the Rule of Law, December 2018, available at <https://theiij.org/wp-content/uploads/Non-Binding-Guiding-Principles-on-Use-of-Battlefield-Evidence-EN.pdf>.

[3] *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings.*

[4] See, for example, Charles Faint and Michael Harris, "OPS/INTEL Fusion Feeds the SOF Targeting Process," *Small Wars Journal*, January 31, 2012, available at <https://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process>.

[5] *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings.*

[6] Ibid.

[7] Esper, "Classification of Materials Captured, Collected, or Handled by the Department of Defense."

[8] Ibid.

[9] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DOD, 2018), available at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[10] Central Intelligence Agency, "CIA Releases Nearly 470,000 Additional Files Recovered in May 2011 Raid on Usama Bin Ladin's Compound," press release and statements, November 1, 2017, available at <https://www.cia.gov/news-information/press-releases-statements/2017-press-releases-statements/cia-releases-additional-files-recovered-in-ubl-compound-raid.html>. See also Combating Terrorism Center at West Point, "Harmony Program," available at <https://ctc.usma.edu/harmony-program/>; Office of the Director of National Intelligence, "Bin Laden's Bookshelf," available at <https://www.dni.gov/index.php/features/bin-laden-s-bookshelf>; Central Intelligence Agency, "November 2017 Release of Abbottabad Compound Material," available at <https://www.cia.gov/library/abbottabad-compound/index.html>.

[11] The term *external operations* refers to terrorist attacks that take place outside a violent extremist organization's safe haven or primary areas of operation. It is distinct from the more traditional term *international terrorism*. For example, al Qaeda affiliate Jemaah Islamiyyah executed an attack against the Australian embassy in Jakarta, Indonesia, in September 2004. This attack falls into the category of international terrorism because the target was the Australian embassy. However, it is not considered an external operation because Islamiyyah is based in Indonesia. Al Qaeda leaders focused their external operations on the so-called far enemy or Western countries.

[12] Office of Public Affairs, Department of Justice, "Al Qaeda Operative Convicted for Role in International Terrorism Plot Targeting the United States and Europe," press release, March 4, 2015, available at <https://www.justice.gov/opa/pr/al-qaeda-operative-convicted-role-international-terrorism-plot-targeting-united-states-and>.

[13] *United States v. Naseer*, 16-373-cr (U.S. Court of Appeals for the Second Circuit, August 20, 2019), available at <www.leagle.com/decision/infco20190820084>.

[14] Office of Public Affairs, Department of Justice, "Man Sentenced for Terrorism-Related Crimes," press release, November 7, 2018, available at <https://www.justice.gov/opa/pr/syrian-man-sentenced-terrorism-related-crimes>. See also Morgan Loew, "Fingerprints Led FBI to Notorious IED Maker," CBS News, November 9, 2018, available at <www.azfamily.com/news/investigations/cbs_5_investigates/fingerprints-led-fbi-to-notorious-ied-maker/article_3be84fc0-e466-11e8-abb0-078163cc8e32.html>.

[15] Ibid. See also U.S. Attorney's Office, Phoenix, Arizona, "Defendant Extradited to the United States to Face Terrorism Charges," press release, August 28, 2014, available at <https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/defendant-extradited-to-u.s.-to-face-terrorism-charges>.

[16] "Turkey Extradites ISIS-Linked Syrian to U.S. on Terror Charges," *Daily Sabah* (Istanbul), September 2, 2014, available at <www.dailysabah.com/mideast/2014/09/02/turkey-extradites-isislinked-syrian-to-us-on-terror-charges>. Other examples also exist. In 2011 in *United States v. Alwan*, the FBI's Terrorist Explosive Device Analytic Center (TEDAC) matched the fingerprints from an improvised explosive device produced in Iraq (around 2005) to a man living in Kentucky. TEDAC has received over 100,000 IED submissions from over 50 countries. See *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings.*

[17] Amandine Scherrer, ed., *The Return of Foreign Fighters to EU Soil, Ex-Post Evaluation* (Brussels: European Parliament Research Service, May 2018), 49, available at <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)621811>; Arthur Martin, Ian Drury, and Martin Robinson, "ISIS Staff List Is Leaked: Names and Family Details of 22,000 Jihadis Revealed in Cache of Application Forms Complete with References (and Next of Kin)," *Daily Mail*, March 10, 2016, available at <https://www.dailymail.co.uk/news/article-3484702/Names-family-details-22-000-jihadis-revealed-huge-cache-leaked-ISIS-HR-forms.html>.

[18] Ibid.

[19] Martin, Drury, and Robinson, "ISIS Staff List Is Leaked."

[20] Europol, *European Union Terrorism Situation and Trend Report 2017* (Brussels: European Agency for Law Enforcement Cooperation, June 15, 2017), 19, available at <https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017>.

[21] Vickiie Oliphant, "Terror Warning: ISIS Files Reveal Danish Recruiters Who 'Plotted Attack' Links to UK," *Express Online*, April 18, 2016, available at <https://www.express.

co.uk/news/world/662217/ISIS-files-Danish-recruiters-linked-to-UK>.

[22] Sajid Javid, "UK Nationals Returning from Syria," presentation before the House of Commons, February 18, 2019, available at <www.theyworkforyou.com/debates/?id=2019-02-18c.1193.0>.

[23] Bibi van Ginkel and Christophe Paulussen, *The Role of the Military in Securing Suspects and Evidence in the Prosecution of Terrorism Cases Before Civilian Courts: Legal and Practical Challenges*, ICCT Research Paper (The Hague: International Centre for Counter-Terrorism, May 2015), available at <https://icct.nl/wp-content/uploads/2015/04/ICCT-Van-Ginkel-Paulussen-The-Role-Of-The-Military-In-Securing-Suspects-And-Evidence-In-The-Prosecution-Of-Terrorism-Cases-Before-Civilian-Courts.pdf>.

[24] Ibid.

[25] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), *Guidelines to Facilitate the Use and Admissibility as Evidence in National Criminal Courts of Information Collected, Handled, Preserved, and Shared by the Military to Prosecute Terrorist Offences* (New York: CTED, January 2020), available at <https://www.un.org/sc/ctc/wp-content/uploads/2020/01/Battlefield_Evidence_Final.pdf>.

[26] Ibid.

[27] While this article focuses on efforts to bring battlefield evidence into civilian courtrooms to minimize threats against the U.S. homeland and the West, it is worth noting that the joint force also has been very much invested in using CEM to mitigate the devastating impact of IEDs on Servicemembers. CEM recovered from a blast site by trained experts (such as explosive ordnance device teams) has enabled the joint force to counter future IED strikes by attacking the insurgent network(s). This has been accomplished by exploiting the acquired CEM and analyzing its derived information and intelligence for biometrics (fingerprints and DNA), the origin of its components, or its explosive composition (military grade, commercial, or homemade), to name a few. Numerous organizations have been involved in these efforts over the past 20 years, including the Joint Improvised Explosive Devise Defeat Organization and the Joint Improvised-Threat Defeat Organization (now called the Defense Threat Reduction Agencies' Directorate of Operations and Integration).

[28] Europol, *European Union Terrorism Situation and Trend Report 2017*; Scherrer, *The Return of Foreign Fighters to EU Soil*, 49; Europol, *European Union Terrorism Situation and Trend Report 2019* (Brussels: European Agency for Law Enforcement Cooperation, June 27, 2019), available at <https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat>; Nathan A. Sales, "After the Caliphate: A New Global Approach to Defeating ISIS," remarks by the Coordinator for Counterterrorism at the Brookings Institution, Washington DC, April 30, 2019, available at <https://www.state.gov/after-the-caliphate-a-new-global-approach-to-defeating-isis/>.

[29] Europol, *European Union Terrorism Situation and Trend Report 2017*; *Scherrer, The Return of Foreign Fighters to EU Soil*, 49; Europol, *European Union Terrorism Situation and Trend Report 2019*; Sales, "After the Caliphate.".

[30] *Summary of the 2018 National Defense Strategy of the United States of America*, 2, 4. Emphasis in original.

[31] Ibid. See also *Description of the National Military Strategy 2018* (Washington, DC: The Joint Staff, 2018), available at <https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf>.

[32] U.S. Central Command, "U.S. Dhow Interdictions," public affairs release, February 19, 2020, available at <https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/2087998/us-dhow-interdictions/>.

[33] Ibid.

[34] Ibid.

[35] "Pompeo Says U.S. Seized Iranian Weapons on Way to Houthi Rebels In Yemen," Reuters, July 8, 2020, available at <www.reuters.com/article/us-usa-iran-pompeo/pompeo-says-un-arms-embargo-on-iran-must-be-extended-to-prevent-further-regional-conflict-idUSKBN2492AV>.

[36] Department of the Treasury, "Treasury Designates Individuals and Entities Involved in the Ongoing Conflict in Ukraine," press release, June 20, 2017, available at <https://www.treasury.gov/press-center/press-releases/Pages/sm0114.aspx>.

[37] Ibid.

[38] Thomas Gibbins-Neff, "How a 4-Hour Battle Unfolded Between Russian Mercenaries and U.S. Commandos in Syria," *New York Times*, May 24, 2018, available at <www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html>.

[39] "UN Monitors Say Mercenaries from Russia's Wagner Group Fighting in Libya," Radio Free Europe, May 7, 2020, available at <https://www.rferl.org/a/wagner-un-russia-libya/30598355.html>.

[40] Ibid.

[41] Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets," press release, July 29, 2019, available at <https://www.justice.gov/opa/pr/texas-man-convicted-conspiracy-commit-theft-trade-secrets>; Meagan Flynn, "Houston Area Engineers Accused of Stealing Trade Secrets to Benefit China's Military," *Houston Press*, May 25, 2017, available at <www.houstonpress.com/news/six-engineers-in-houston-charged-in-plot-to-steal-trade-secrets-to-benefit-china-9467242>.

[42] Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets"; Flynn, "Houston." See also Office of Public Affairs, Department of Justice, "Two Businessmen Charged with Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company," press release, April 27, 2018, available at <https://www.justice.gov/opa/pr/two-businessmen-charged-conspiring-commit-economic-espionage-benefit-chinese-manufacturing>; Spencer Hsu, "Houston Businessman Convicted of Conspiring to Steal Trade Secrets, Acquitted of Economic Espionage for China," *Washington Post*, July 29, 2019, available at <www.washingtonpost.com/local/legal-issues/houston-businessman-convicted-of-conspiring-to-steal-trade-secrets-acquitted-of-economic-espionage-for-china/2019/07/29/92418df2-b245-11e9-8f6c-7828e68cb15f_story.html>; *United States v. Shan Shi*, 2019 U.S. Dist. Lexis 218100 (United States District Court for the District of Columbia, December 17, 2019, Filed), available at <www.lexislegalnews.com/articles/46649/judge-rejects-acquittal-bid-by-defendant-in-trade-secret-theft-suit>.

[43] Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets"; Flynn, "Houston." See also Office of Public Affairs, Department of Justice, "Two Businessmen Charged with Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company"; Hsu, "Houston Businessman Convicted of Conspiring to Steal Trade Secrets, Acquitted of Economic Espionage for China"; *United States v. Shan Shi*.

[44] Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets"; Flynn, "Houston." See also Office of Public Affairs, Department of Justice, "Two Businessmen Charged with Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company"; Hsu, "Houston Businessman Convicted of Conspiring to Steal Trade Secrets, Acquitted of Economic Espionage for China"; *United States v. Shan Shi*.

[45] DOD defines *instruments of national power* thus: "All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational and military." See Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, July 12, 2017), available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2019-02-11-174350-967>.

NDU Press Congratulates the Winners of the 2020 Essay Competitions

NDU Press virtually hosted the final round of judging in May 2020, during which 26 faculty judges from 14 participating professional military education (PME) institutions selected the best entries in each category. There were 72 submissions in this year's three categories. First Place winners in each of the three categories appear in the following pages.

Secretary of Defense National Security Essay Competition

The 14th annual competition was intended to stimulate new approaches to coordinated civilian and military action from a broad spectrum of civilian and military students. Essays address U.S. Government structure, policies, capabilities, resources, and/or practices and to provide creative, feasible ideas on how best to orchestrate the core competencies of our national security institution.

First Place (tie)
Lieutenant Colonel Roderick K. Butz, USAF
U.S. Army War College
"Beneath the Crosshairs: Remotely Piloted Airstrikes as a Foreign Policy Tool"

First Place (tie)
Kaleb J. Redden, Office of the Secretary of Defense
National War College
"Competition Is What States Make of It: A U.S. Strategy Toward China"

Second Place
Kyle Richardson, Department of State
National War College
"Indonesia: Lessons for the U.S.-China Geo-Economic Competition"

Third Place
Lieutenant Colonel Eric V.M. Kreitz, USA
U.S. Army War College
"Re-Emerging Russian Influence in Latin America and U.S. Foreign Policy Response"

Chairman of the Joint Chiefs of Staff Strategic Essay Competition

This annual competition, in its 39th year in 2020, challenges students at the Nation's joint PME institutions to write research papers or articles about significant aspects of national security strategy to stimulate strategic thinking, promote well-written research, and contribute to a broader security debate among professionals.

Strategic Research Paper

First Place
Lieutenant Colonel Jeremy McKissack, USAFR
Air War College
"Pardon the Paradox: Making Sense of President Trump's Interventions in Military Justice"

Second Place
Lieutenant Colonel Matthew Kendrick Mulvey, USMC
U.S. Naval War College (Senior)
"Helping Hanoi Keep the Dragon at Bay in the South China Sea"

Third Place
Amy C.F. Carlon, Department of State
Eisenhower School of National Security and Resources Strategy
"Diplomatic Engagement on Missile Defense Amidst Great Power Competition"

Strategy Article

First Place
Colonel Mark M. Zais, USA
U.S. Army War College
"Artificial Intelligence: A Decisionmaking Technology"

Second Place
Lieutenant Colonel Kukunaokala (Kuna) Mendonca, ARNG
U.S. Army War College
"Cybersecurity Initiatives in the National Guard: Opportunities and Challenges"

Third Place
Lieutenant Colonel Jeremy McKissack, USAFR
Air War College
"First Among Equals: Diplomacy as America's Primary Instrument of Power"

Joint Force Quarterly Maerz Awards

In its 5th year, the *JFQ* Maerz Awards, chosen by the staff of NDU Press, recognize the most influential articles from the previous year's four issues. Five outstanding articles were chosen for the Maerz Awards, named in honor of Mr. George C. Maerz, former writer-editor of NDU Press.

Forum
Glenda Jakubowski
"What's Not to Like? Social Media as Information Operations Force Multiplier," *JFQ* 94 (3rd Quarter 2019)

JPME Today
Dale C. Eikmeier
"Simplicity: A Tool for Working with Complexity and Chaos," *JFQ* 92 (1st Quarter 2019)

Commentary
Jeffery Zust and Stephen Krauss
"Force Protection from Moral Injury: Three Objectives for Military Leaders," *JFQ* 92 (1st Quarter 2019)

Features
Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden
"Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *JFQ* 92 (1st Quarter 2019)

Recall
John K. DiEugenio and Aubry J. Eaton
"Flanking the Crater," *JFQ* 94 (3rd Quarter 2019)

Joint Doctrine
J. Mark Berwanger
"Fire for Effect: The Evolution of Joint Fires," *JFQ* 93 (2nd Quarter 2019)

Distinguished Judges

Twenty-six senior faculty members from the 14 participating PME institutions took time out of their busy schedules (and online teaching duties) to serve as judges for this year's competitions. Their personal dedication and professional excellence ensured strong and credible competitions.

The judges were Joseph L. Billingsley, College of Information and Cyberspace; Brandy Lyn Brown, Marine Corps University; Mark A. Bucknam, National War College; Dr. Charles Chadbourne, U.S. Naval War College; Dr. James Chen, College of Information and Cyberspace; Dr. Benjamin "Frank" Cooling, Eisenhower School of National Security and Resources Strategy; Dr. Armando DeLeon, Air University eSchool of Graduate PME; Dr. Richard L. DiNardo, Marine Corps Staff College; Dr. Peter Eltsov, College of International Security Affairs; Dr. Jack Godwin, NDU Press; Dr. Todd Holm, Marine Corps University; Dr. C.J. Horn, Air Force Cyber College; Dr. James D. Kiras, School of Advanced Air and Space Studies; Captain Bill Marlowe, USN (Ret.), Joint Forces Staff College; Dr. Brian McNeil, Air War College; Dr. Larry D. Miller, U.S. Army War College; Dr. Kristin Mulready-Stone, U.S. Naval War College; Dr. Jaimie Orr, National War College; Dr. Nicholas M. Sambaluk, Air University eSchool of Graduate PME; Jesse P. Samluk, National Intelligence University; Dr. Nicholas E. Sarantakes, U.S. Naval War College; Dr. Naunihal Singh, U.S. Naval War College; Dr. Paul Springer, Air Command and Staff College; Dr. Jeff Turner, Joint Forces Staff College; Dr. David A. Wigmore, College of International Security Affairs; and Dr. Elizabeth D. Woodward, Air War College.