The University of Maryland, College Park

Examinations of Saudi-Iranian Gray Zone Competition in MENA, and of Potential Outcomes of the Flow of Foreign Fighters to the United States.

A Report on Three ICONS Simulations

Strategic Multilayer Assessment Support to U.S. Special Operations Command (SOCOM) and the DHS S&T Office of University Programs

November 2016

About This Report

The authors of this report are:
Ron Capps, Researcher and Simulation Developer, ICONS
Devin Ellis, Policy and Research Program Director and Lead Simulation Developer, ICONS
Jonathan Wilkenfeld, Director, ICONS

Questions about this report should be directed to Devin Ellis at ellisd@umd.edu.

This research was supported by the U.S. Department of Defense Joint Staff; J39 through Award Number 2012-ST-061-CS0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Defense, U.S. Department of Homeland Security.

About the ICONS Project

The ICONS Project creates simulations and scenario-driven exercises to advance participants' understanding of complex problems and strengthen their ability to make decisions, navigate crises, think strategically, and negotiate collaboratively.

About START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is supported in part by the Science and Technology Directorate of the U.S. Department of Homeland Security through a Center of Excellence program led by the University of Maryland. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and social and psychological impacts of terrorism. For more information, contact START at infostart@start.umd.edu or visit www.start.umd.edu.

Citation

To cite this report, please use this format:

Capps, Ron; Ellis, Devin and Wilkenfeld, Jon . "Examinations of Saudi-Iranian Gray Zone Competition in MENA, and of Potential Outcomes of the Flow of Foreign Fighters to the United States," Report to DoD Strategic Multilayer Assessment Branch; Support to USSOCOM. College Park, MD: START, 2016.

Contents

Examinations of Saudi-Iranian Gray Zone Competition in MENA, and of Potential Outcomes of the Flow of Foreign Fighters to the United States

Executive Summary

The United States is regularly challenged by the actions of states and non-state actors in the nebulous, confusing, and ambiguous environment known as the Gray Zone. Planners, decision makers, and operators within the national security enterprise need to understand what tools are available for their use in the Gray Zone and how to best develop, employ, and coordinate those tools. This report summarizes the results of simulations created and executed by the ICONS Project as part of a larger study to capture at least some of the information needed toward that end.

On October 24, 26, and 28, 2016, under the guidance of the Pentagon's Office of Strategic Multi-Layer Assessment and the Department of Homeland Security's Office of University Programs, staff of the ICONS Project at the University of Maryland executed three simulations. Two of these examined competition between Iran and Saudi Arabia in the Gray Zone, both direct and through proxies. The third examined the threat to the homeland of a collapse of Islamic State in Iraq and Syria.

Participants in the simulations were drawn from various U.S. government agencies and from universities, research centers, think tanks, foreign governments and militaries. Within each of the three simulations participants were given start states and asked to react to events introduced into the scenario. Broadly, the start states placed the participants in mid-2017, about six months into a new U.S. administration. They were told the USG had placed a priority on understanding and shaping the relationship between Iran and Saudi Arabia (in two of the simulations) or in understanding and protecting the homeland against any threat evolving from the competition between Islamic State and Al Qaida (in the third). Play in each of the simulations took place virtually with participants joining via ICONSnet from around the world. Each of the three simulations ran for four hours.

There were five principal take-aways from these simulations:

— It may not be possible for the U.S. to influence or shape Gray Zone activities by other states, especially when those actions are not directed toward the United States. When two states or a mix of state and non-state actors want to engage in the Gray Zone, there may be little the U.S. can do to stop them. Sometimes the only possible action is no action other than planning for likely results.

—Violent extremist organizations may act in the Gray Zone in an attempt to drag state actors out of the Gray Zone. State actors need to have appropriate strategies developed and responses queued for rapid delivery.

— The U.S. is not the sole major power assessing threats and opportunities in Gray Zone conflicts and competitions. It is possible that actions by other major powers could draw the U.S. further into conflicts or drive parties to violence.

— To operate effectively in the Gray Zone, U.S. policy designers and operators need access to every available tool; a whole-of-government approach is crucial to success. In fact, we should begin to think in terms of a whole-of-government-plus structure where government reaches out to non-government regional and technical specialists, subject matter experts, and other "different thinkers" to formulate courses of action.

— Controllers noted a clear bias among the U.S. government participants toward Saudi Arabia and against Iran, and a willingness to move rapidly to kinetic or other military action by some of the military

players. Such an overt bias may adversely affect the ability of the U.S. to take advantage of opportunities for influence in Gray Zone conflicts.

Participants in the Iran-Saudi Arabia simulations stated in after action reviews their belief that the U.S. must recruit, train, and deploy the right people with the right skills, including a mix of government and non-government thinkers. There was also a note that the USG lacked a cabinet level information agency dedicated to developing and disseminating the U.S. narrative and to countering enemy narratives.

In their after-action reviews, participants in the foreign fighter scenario focused on the difficulties of developing and maintaining a common operating picture across federal, state, and local entities; on the importance of understanding the roles, capabilities, and authorities of each entity; on the importance of accurate and timely intelligence, and how to share information to best effect across agencies where security clearance levels vary.

Introduction

Concept and Purpose: Consider Response Options Against Gray Zone Conflicts.

The ICONS Project, a part of the Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, was asked to design and execute a simulation exploring response options to potential Gray Zone conflicts in the Middle East/North Africa region (MENA). This work was part of a collaborative effort between the Office of Strategic Multilayer Assessment (SMA) at the Joint Staff J39, U.S. Special Operations Command (USSOCOM), and the Department of Homeland Security (DHS). The MENA scenario was one of three scenarios developed for examination of Gray Zone threats; the others involved Russia and China.

The primary objective of the activity was to explore the capabilities needed for maneuver against destabilizing actors in the MENA region in the Gray Zone and to identify how different elements of U.S. power should be utilized and coordinated to respond to trans-regional threats with multi-domain responses. During the development of the simulation, designers and the leadership of SMA, USSOCOM, and DHS determined that ICONS would develop and execute three separate simulations.

Report Contents, Simulation Structures, and Caveats

The Report covers the key elements considered in the design and execution of these simulations, as well as the details of the scenarios, and a summary of key findings from the exercises.

Two simulations were primarily focused on the Gray Zone competition between Saudi Arabia and Iran both direct and through proxies; the third examined the potential for attacks in the United States resulting from competition between Al Qaida and Islamic State and involving returned foreign fighters, homegrown, and self-radicalized terrorists. Sections of this report will highlight details of each of the three simulations developed for this task.

The scenarios and subsequent updates and injects do not reflect the opinion of the Departments of Defense or Homeland Security, or the U.S. government. Neither this report nor any report prepared under the auspices of SMA and DHS contain policy recommendations for the U.S. government.

Simulation Design

Scenario Development

Given the medium term time horizon for the simulation and the desire to allow for maximum creativity and divergence in the decision making of the actors, the designers had two significant conceptual challenges: (1) what is thought of as "chasing the news," that is working to stay ahead of the creativity and activities of the state and non-state actors in the region, and (2) the 2016 presidential elections in the U.S. (The simulations were conducted less than two weeks before the general election.)

The designers chose two broad narrative paths: Saudi and Iranian competition in the Gray Zone, and the potential threat of foreign fighter returns to the U.S. following a collapse of Islamic State in Syria and Iraq. Simulations run on Monday October 24 and Wednesday October 26 were principally focused on the Gray Zone competition between Iran and Saudi Arabia (IR-SA). The simulation run on Friday October 28 focused on the threat to the homeland from returning foreign fighters (FF). The scenarios were developed in consultation with key leaders from Strategic Multilayer Assessment project teams and a team of subject matter experts.

Actors

Rather than specify that role players be drawn from certain U.S. government agencies, SMA asked the designers to identify skills and expertise needed within the simulations.

IR-SA: Within the two IR-SA simulations, skills and expertise needed were:

—diplomacy (bi-lateral, multi-lateral, and through International Organizations);
—international economics;
—international finance and sanctions;
—international arms trade;
—information and influence operations;
—law of the sea and laws of war;
—international humanitarian law;
—operating authorities under UN Security Council Resolutions;
—U.S. law and policy regarding claims of asylum and refugee status;
—operational level military operations;
—cyber-war and cyber security.

FF: During the foreign fighter simulation, the skills and expertise needed were:

—protection of the homeland;
—coordination of federal law enforcement activities;
—cooperation among federal, state, and local officials,
—intelligence analysis;
—dissemination and management of intelligence reporting;
—civ-mil coordination;
—public affairs, media analysis, and media response.

During both the IR-SA and FF simulations, participants worked on a team identified as Blue. During the two IR-SA simulations, Blue was a single element within which government and non-government actors fused their knowledge to identify and develop potential courses of action in response to the scenario and additional injects. During the FF simulation, Blue was divided into teams representing Federal Law Enforcement Agencies (FLEA), the Intelligence Community (Intel), a Press and Public Affairs office (PAO), and a team serving as liaisons to regional fusion centers (LNO). The additional challenge for Blue during the FF simulation was to communicate among the four sub-teams (sharing tightly stove-piped information) in order to identify threats, recommend courses of action and maintain a common operating picture.

One of the main goals of conducting an unclassified exercise of this nature is to bring expertise and perspectives from outside the U.S. government national security agencies to bear. Every effort was made to have subject matter experts with deep backgrounds and personal experience with the relevant actors on each team, with the goal of bringing to bear deeper and more nuanced thinking than is often available in a more restricted, classified environment.

Mechanics: Iran and Saudi Arabia Simulations

Within the context of the two IR-SA simulations, the principal actors—Saudi Arabia and Iran—were not acting directly against the U.S., but rather (on day one) against one another or (on day two) acting through proxies to achieve strategic ends. The play began with a "start state" and continued with event injects that presented either a phenomenon or an event and then tracked the aftermath or follow-on actions taken by the actors or other state or non-state actors, including the USG.

In effect, Blue was reacting to a series of events and phenomena within the diplomatic, economic, information, cyber, and legal arenas, along with attacks or threats to infrastructure, culture and religion, societal norms, and more. Once play began and injects flowed, players had an opportunity for *synchronous communication* where they could approach other actors with proposals, diplomatic efforts, planning among allies, etc.

During these simulations, the control team had access to an *analytic support team* (identified here as Red) comprised of members of the project team supporting the larger Strategic Multilayer Assessment, and a group of international military officers.

Mechanics: Foreign Fighters Simulation

In the foreign fighters simulation the principal actors (Al Qaida and Islamic State) took actions directly targeting the U.S. Play began with a "start state" and continued as the four Blue sub-teams were confronted with events and phenomena which the sub-teams (federal law enforcement, public affairs, intelligence, and liaison) had to react to and keep other groups informed of.

The play was essentially a series or puzzles or mysteries that the players needed to solve in an effort to stop specific attacks on the homeland. There were, of course, additional complications ranging from intelligence failures to sectarian violence and lone-wolf attacks. As the scenario spooled out in this simulation the time between major events shortened and the geographic spread of events broadened.

Throughout this simulation, Control had access to an *analytic support team* (identified here as Red) comprised of members of the project team supporting the larger Strategic Multilayer Assessment.

Exercise Structure

The simulations ran over the course of five days, October 24-28 2016. In order to facilitate participation from a diverse group of subject matter experts over a relatively long time commitment, the decision was made to run the simulation as a distributed exercise over the ICONS proprietary online platform, ICONSnet. Participants were located throughout the greater Washington, DC area, as well as in Tidewater VA, Kansas, Florida, Nebraska, North Carolina, Rhode Island, Texas, Canada, Iraq, Qatar, and Great Britain.

Exercise Schedule

Participants were offered a thirty-minute introduction to ICONSnet in the days immediately prior to the simulations. The control team also made available the initial states for the scenarios and a set of participant instructions. On each day the simulation went live at 0800 (EDT) and ended at 1200 (EDT). In each simulation there were two rounds of play, each ninety minutes long and separated by a fifteen-minute break. At 1130 play stopped in order to allow players the opportunity to conduct an online hotwash based on questions posed by the controllers.

—Monday, October 24, 2016: Gray Diplomacy. Iranian and Saudi efforts to gain influence at the expense of the other in the diplomatic and economic arenas and in the court of public opinion.

—Wednesday, October 26, 2016: Proxy Wars. Saudi and Iranian conflict plays out in Yemen and Bahrain with both parties' adventurism and use of proxies stretching the limits of Gray Zone activities.

—Friday, October 28, 2016: Foreign Fighters. ISIS collapse in Syria and Iraq brings Islamic State and Al Qaida to America.

ICONSnet Platform

ICONSnet is a web-based platform with a database backend, accessible through any internet browser. Each simulation run in ICONSnet is in a distinct "community" which remains in place after the exercise, capturing a record of proceedings for future review and analysis.

Communication Mechanisms (Messaging and Conferencing)

Participants in the simulation are able to communicate within and across teams using the ICONSnet messaging and conferencing functions. The messaging system works in a similar fashion to email, enabling participants to compose, reply to, and forward messages. In addition, participants could join conferences, which operate like chat rooms, to hold meetings. During these simulations, each team conducted internal deliberations and meetings in a team conference. They communicated with other actors through messaging, or by inviting them to a new conference to meet on specific topics with the relevant parties.

Scenarios: Iran-Saudi Arabia Simulations

Day One: Gray Diplomacy

Start State

It is mid-2017. You've been asked to join a U.S. government task force studying the ongoing competition between Iran and Saudi Arabia. Relations between these two Middle East giants have recently worsened. Iran appears ascendant in the wake of the release of billions of dollars formerly locked up by the United States, and following the end of most U.S., European, and other international sanctions. Saudi Arabian leaders feel challenged on several fronts: internally by protests against the monarchy, and externally by what they view as an existential threat from an increasingly powerful and aggressive Iran. Saudi bombing of targets both civilian and military in Yemen continues. Iranian support for Shia people and movements worldwide is increasing.

Elections in France last month brought Alain Juppe and *Les Républicains* to power in a very tight race against Marine LePen and the *Front National*. German federal elections are scheduled to take place in six weeks. Across Europe right-wing, nationalist, and isolationist parties are gaining strength and confidence.

The new U.S. president faces challenges from both sides of the aisle and there is a simmering discontent across the U.S. with the result of the 2016 election and the new president's policies. The president is concerned about the stability of the Middle East, lest some catastrophe draw the U.S. into a (another?) conflict there. The president and the national security advisor believe that the competition between Saudi Arabia and Iran is a significant destabilizer. So, the national security advisor has formed an ad hoc virtual task force to "sort out the competition between Iran and Saudi Arabia and keep it from boiling over into potentially catastrophic and lethal conflict."

The national security advisor has told the members of the task force, "Let's not allow the president to be surprised by anything happening between the Saudis and Iranians. When something is going on between these two, let me know—and not just what's happening but also what our position should be and what options we can offer to POTUS. The president isn't afraid to take charge, and will personally

direct actions down to whatever level is necessary. So don't be afraid to suggest actions well below the strategic level and across multiple domains."

Participant Instructions

During this simulation you will receive messages from the intelligence community, the Departments of State and Defense, the media, and others. Among the members of the task force (known here as Blue), discuss the situations described and any potential reactions or threats to the U.S. or our allies. When something happens or looks like it might happen, be prepared to advise the national security advisor (known here as simcon) on a recommended course of action, which might be anything from do nothing to continue to observe to launch aircraft. Be prepared to explain why you think this is the best course of action and what the potential result might be—both positive and negative.

Synopsis of Events During the Gray Diplomacy Simulation

In this scenario Iran and Saudi Arabia are deeply engaged in Gray Zone competition across the DIMEFIL spectrum. During a speech at the United Nations, the Iranian president proposes the Middle East become a WMD-Free zone, challenging Israel and Saudi Arabia to destroy any and all WMDs each holds—and offering to lead the way by destroying its own chem-bio weapons programs. The Saudis demur and opt to expand their nuclear power program and to secretly pursue nuclear parity with Israel and Iran.

Saudi Arabia announces it will make an initial public offering of shares of Saudi Aramco and makes the release day a Sunni holy day. An unknown entity hacks into Aramco's servers and downloads an enormous amount of financial data that, if it is released, could damage the corporation's standing in the days immediately prior to the IPO. The data is provided to the Financial Time and the Saudis sue FT attempting to stop the publication, but a judge rules the case to be without merit. The FT publishes the data; Wikileaks publishes a second tranche days later.

Iran joins the Shanghai Cooperation Organization and invites the other members to take part in a large scale war game the following year in Iran. Three Chinese combatant ships visit Iran to publicize the licensing of production of a Chinese amphibious transport ship in Iran in return for reduced natural gas prices for the Chinese. Russia sells Iran 200 main battle tanks, in retaliation (it is rumored) for the U.S. sale of M1 tanks to Saudi Arabia and a massive ammunition sale to the United Arab Emirates.

On the internet a slickly produced show appears detailing the lives of three families in what can only be Saudi Arabia: one rich, one middle class, and one struggling. The show paints the rich family—loosely connected to the Saudi royal family—in a very negative light. The show is wildly popular (and banned) in Saudi Arabia.

Iran announces a deal with Turkey to build a pipeline linking Iran's oil fields with seaports in Turkey, shortening the distance to Europe for Iranian petroleum.

Saudi Arabia calls on the Financial Action Task Force to keep Iran on the Blacklist. Iran retaliates by referring Saudi Arabia to the International Criminal Court for war crimes committed in Yemen and documented in a United Nations report. The British and German parliaments cease all arms sales and transfers to Saudi Arabia and pressure mounts for the U.S. to do the same. The Saudi king calls in the U.S. ambassador to discuss it.

Wikileaks releases a trove of documents purporting that a Saudi bank has been supporting Al Qaida. Salted throughout this data are documents that prove the U.S. has this information and has done nothing about it. It is unclear if the documents are real or spurious.

Day Two: Proxy Wars

Start State

It is mid-2017. You've been asked to join a U.S. government task force studying the ongoing competition between Iran and Saudi Arabia. Relations between these two Middle East giants have recently worsened. Iran appears ascendant following the release of billions of dollars formerly locked up by the United States, and the end of most U.S., European, and other international sanctions. Saudi Arabian leaders feel challenged on several fronts: internally by protests against the monarchy, and externally by what they view as an existential threat from an increasingly powerful and aggressive Iran. Saudi bombing of targets both civilian and military in Yemen continues. Saudi support for the al Khalifa monarchy in Bahrain is unwavering. Iranian support for Shia people and movements worldwide is increasing.

Elections in France last month brought Alain Juppe and *Les Républicains* to power in a very tight race against Marine LePen and the *Front National*. German federal elections are scheduled to take place in six weeks. Across Europe right-wing, nationalist, and isolationist parties are gaining strength and confidence.

The new U.S. president faces challenges from both sides of the aisle and there is a simmering discontent across the U.S. with the result of the 2016 election and the new president's policies. The president is concerned about the stability of the Middle East, lest some catastrophe draw the U.S. into a (another?) conflict there. The president and the national security advisor believe that the competition between Saudi Arabia and Iran is a significant destabilizer. So, the national security advisor has formed an ad hoc virtual task force to "sort out the competition between Iran and Saudi Arabia and keep it from boiling over into potentially catastrophic and lethal conflict."

The national security advisor has told the members of the task force, "Let's not allow the president to be surprised by anything happening between the Saudis and Iranians. When something is going on between these two, let me know—and not just what's happening but also what our position should be and what options we can offer to POTUS. The president isn't afraid to take charge, and will personally direct actions down to whatever level is necessary. So don't be afraid to suggest actions well below the strategic level and across multiple domains."

Participant Instructions

During this simulation you will receive messages from the intelligence community, the Departments of State and Defense, the media, and others. Among the members of the task force (known here as Blue), discuss the situations described and any potential reactions or threats to the U.S. or our allies. When something happens or looks like it might happen, be prepared to advise the national security advisor (known here as simcon) on a recommended course of action, which might be anything from do nothing to continue to observe to launch aircraft. Be prepared to explain why you think this is the best course of action and what the potential result might be—both positive and negative—because you are actually, through the national security advisor, presenting courses of action to the president. Be pro-active. Form subgroups if you like based on specialties. Aggressively seek guidance or clarification from higher if you need it. Share thoughts and ideas among the group, form and shape opinions, develop courses of action and push those recommendations up the chain.

Synopsis of Event During the Proxy Wars Simulation

This simulation takes place primarily in Yemen and Bahrain where Saudi Arabia and Iran may be acting through proxies. In Yemen, the Saudi-led anti-Houthi military coalition attempts to profit from a dispute among leaders of Al Qaida in the Arabian Peninsula and the coalition's forces turn to fight AQAP.

Simultaneously, Houthi forces divide their activities and attack AQAP as well. The Houthi government approaches the Omani government in an attempt to have the Omanis serve as a clearinghouse for tactical information between the Houthis and the Saudis in their "joint fight against AQAP." Independent and social media condemn the U.S. for supporting the Saudi attacks on civilians.

In the Gulf of Aden the U.S. Navy intercepts a stateless dhow ferrying a small shipment of arms and confiscates the arms under UNSCR 2216. Iran protests and announces the shipment was destined for "the popular government" in Sanaa which is attacking AQAP. Iran further specifies that in the future all of its arms shipments to the popular government in Sanaa will be escorted by Iranian Navy combatants.

During a ground clash in Yemen, two American citizens engaged in the fighting are captured by the Houthis. During a press event in which a video of the men speaking and declaring they are well and not being mistreated, the Houthis claim the men are U.S. Navy SEALs and demand to know why the U.S. military is engaged on the ground in Yemen. A quick survey of CENTCOM, SOCOM, and the CIA determines that no U.S. military or CIA ground branch operators are missing. The men, Fox News announces, are former U.S. Navy SEALs now engaged by Blackwater/Xe as contractors working for the Saudis. The Houthi government considers the fact that they are former SEALs working for Blackwater instead of active duty SEALs a distinction without a difference.

What is likely a C-802 missile fired from Houthi controlled areas in Yemen sinks an Emirati corvette on routine patrol in the Red Sea. At about the same time, two Iranian ships depart Bushehr for Yemen. One is a frigate the other a cargo vessel.

A Yemeni political group approaches the UN SRSG with a proposal to return Yemen to the status quo ante 1990, in effect dissolving the construct of Yemen and returning to two Yemens: North and South. Iran offers to support a UN peacekeeping mission to separate the combatant parties.

In Bahrain, a likely government slight toward Shia Muslim citizens brings the Shia back to the streets in protests. Old women form the front lines of the protests, forcing the Bahraini military to use force against old women in order to maintain what it views as order. A foreign intelligence service provides the U.S. with some evidence that the Iranians are behind in the protests.

The protests grow in frequency and size including demonstrations in front of the Naval base in Manama. Other groups join including a group of 100 Shia clerics who appear to have the support of some Sunni groups in calling for a more democratic Bahrain. There is a surge of social media reporting on the protests that the government of Bahrain cannot overcome. Images circulate around the world of Bahraini troops beating old women. The government is under a great deal of pressure to stop the protests.

Saudi Arabia prepares to intervene (again) in Bahrain militarily and independent media shows images captured by either a satellite or drone of the Saudi mobilization. During a storm, in what may be an act of God or may be covert action by Iranian Quds Force, a ship breaks the causeway linking the mainland and the island. When the U.S. needs to bring a combatant ship into the Naval Base in Manama for emergency repairs following the storm, anti-government websites begin to suggest that the U.S. is coming to support the king because the Saudis cannot.

The government moves to round up the leaders of the protests. At both the U.S. embassy and the naval base, groups of protestors begin to ask for asylum having fully demonstrated a well-founded fear of persecution.

Day Three: Foreign Fighters

Start State

It is mid-2017. You are a member of an ad hoc virtual task force formed by the recently inaugurated president of the United States to study, monitor, and be prepared to react to the evolving global jihad now that Islamic State has been defeated in Iraq and Syria. Members of the Task Force

include representatives from various federal law enforcement agencies, the intelligence community, a public affairs and media analysis team, and a team working in liaison with the numerous fusion centers around the country.

The director of the task force has chosen a "fusion cell" approach to its work in which representatives of various agencies work together to identify targets, design potential courses of action, and task operators. She is particularly keen on vertical as well as horizontal information integration: from global to regional to national, and among federal, state, and local governments and entities. As a members of the task force you are encouraged share information, to create new relationships and networks of agencies, organizations, and groups.

Naturally, USG security classification rules remain in effect; so sharing intelligence will be a challenge. Representatives of the intelligence community have clearance and need to know for Top Secret information. Everyone else on your team has clearance and need to know for Secret level information. State and local officials with whom you may communicate (through regional fusion centers, for example) are not yet cleared for U.S. government classified information. Also, the task force is a newly formed entity and not everything works perfectly, yet.

The collapse of Islamic State (IS) has amplified the movement, realignment, and reconsolidation of foreign fighters and of organized terrorist fighting units. IS leadership remain committed to infiltrating terrorists into Europe and the United States, as well as in inspiring, recruiting, and developing home-grown and self-radicalized terrorists.

Al Qaida (AQ) strives to regain primacy among jihadi groups and has recently sought to bring Islamic State adherents to AQ as IS has stumbled. There have been numerous defections from IS to AQ. Some analysts have written that AQ leadership is planning a major terror attack—perhaps on infrastructure or a symbolic religious target—to help re-establish the organization's preeminence.

Disagreements between Turkey and the European Union (as well as among individual European nations) have led to a functional collapse of the 2016 deal to return migrants to Turkey from the Mediterranean Sea or Greece, and as a result migrants have again begun to arrive in Greece. The Socialists were crushed in the recent French presidential elections, not making it past the first round of voting. In the final round, Alain Juppe and *Les Républicains* narrowly defeated Marine LePen and the *Front National*, chilling the left and emboldening the right and hard/far right. Across Europe, and particularly in the east, hard right parties are ascendant. German federal elections will take place in two months.

At home, the new U.S. president faces challenges from both sides of the aisle and across the U.S. there is a simmering discontent with the result of the 2016 election and the new president's policies. This discontent could bubble over into violence committed by groups associated with the left or the right. Add to this the very real threat of both foreign and domestic terrorism sponsored or inspired by Islamic State or Al Qaida and we have a particularly volatile environment in which to operate.

Participant Instructions

Each player has been assigned to a team: either Federal Law Enforcement Agencies (FLEA), Public Relations and Media Analysis (Media), the Intelligence Community (Intel), or liaisons to local and regional law enforcement and fusion centers (LNO). Each team will receive message traffic germane to that team function. No other team will receive that traffic—remember, this is a new organization and not everything works perfectly yet. So teams will have to circulate messages among the other units in the task force to insure situational awareness across unit boundaries.

Classification rules apply, so for the intelligence community, if there is any traffic classified above Secret, you'll have to make decisions on how and what you can share about that message in order to make sure no critical information slips through.

If you have questions, query the boss (known here a simcon). If you need more information about a message you've received, ask simcon. If you want to share information outside the task force, say, with a fusion center or an outside cabinet level department, you can send them a message through simcon.

Once you begin receiving message traffic, the game is live. We'll run for about 90 minutes or so, take a break and then complete the simulation in a final session of about 90 minutes.

Team notes:

The Federal Law Enforcement Agencies. Your team is made up of representatives from various federal law enforcement agencies, some from the Department of Justice, and some from the Department of Homeland Security. You role on the task force is to apply your law enforcement expertise and experience in keeping track of the developing situations the task force follows, keeping your colleagues informed of events that you learn of through message traffic, offering potential courses of action when the situation requires a response.

The Intelligence Community. Your team will serve as the gatekeepers of information drawn from the sixteen (or more) agencies and departments that make up the IC. You'll receive message traffic from across the full spectrum of collectors including sigint, imint, humint, and from liaison agencies (meaning foreign intelligence services with whom we have agreements to share information). Your biggest challenge in some cases will be to find ways to share information (that might be critical to halting a potential event) with law enforcement operators who don't have clearances. At other times, you'll be called upon to analyze and synthesize information provided to you by colleagues on the task force with highly classified processed intelligence to come up with a bit of your own (predictive) analysis.

The Public Affairs and Media Analysis Office. Your tasks include monitoring news reports to remain a constant vigil on open source threat reporting, watching social media for important themes that may serve as indicators for action or policy changes by allies or enemies, advise other members of the team on any necessary responses and, perhaps, draft those responses. So much of what happens is reported first by the media, you'll find that you (rather than the intelligence community) may be the first to know of some ongoing event. It's critical that you're kept in the loop by your teammates in case you have to respond to a media query.

The Liaison Office to Regional, State, and Local Law Enforcement and Fusion Centers. Your office's role is to monitor reports from across the country for activity that might point to some pending terrorist event or for information that others in the LE community need in order to best protect the homeland. You'll want to share your information as broadly as possible within the task force without needlessly flooding your colleagues' inboxes. You should follow up with fusion centers on their reporting if you want more information or need clarification.

Synopsis of Events During the Foreign Fighters Simulation

Islamic State has been defeated in Iraq and Syria and is struggling to recover. Without land to occupy, the Caliphate is null. So the IS leadership yearns to transform into a cyber-Caliphate and is encouraging supporters to fight wherever they are—including the United States. Al Qaida leadership sense an opportunity to re-gain the summit of violent jihadism and urges disillusioned IS members to join the true jihad. Ayman al Zawahiri has urged AQ supporters to continue to fight against the far enemies, Israel and the United States. Both IS and AQ develop and engage plans for attacks in the U.S.

Two Al Qaida operators travel on valid French passports to enter America under the visa waiver program. Only after the men have entered the U.S. does the intelligence community learn that they are on a French intelligence watch list. The men obtain false documentation and electronic access to funds

through a small bank owned by a Saudi citizen—which is under surveillance by the Department of the Treasury. The men separate and go off to execute their respective tasks.

One man goes to St Louis where he joins a returned American citizen who fought with Al Shabaab in Somalia and then trained with AQ in Afghanistan. The other goes to Dallas to find a self-radicalized American who has linked to AQ through jihadi chat rooms. These men then set their plans in motion.

Meanwhile, in Detroit, Scranton, Washington DC, and other cities individual (lone wolf) acts of violence are carried out by radicalized individuals who have pledged allegiance to Islamic State. The Detroit attacks (four small bombs and a last-stand suicide attack on police) spark retaliation attacks against innocent Muslims (multiple murders in Mosques and Islamic centers) by White Supremacists and other anti-Muslim and anti-immigration nationalist groups in numerous cities and town around southern Michigan. Following these attacks the governor mobilizes the National Guard and declares a curfew, further stipulating that anyone seen with a weapon will be considered a threat. These actions are interpreted by alt-right anti-government groups in Michigan and around the country as a declaration of martial law and de facto repeal of the second amendment. Numerous alt-right groups mobilize including Three-Percenters, Oath Keepers, Sovereign Citizens, and the Michigan Militia. Across the country, as White supremacist and nationalist groups stand up they are matched by Black group ranging from church groups to Black Lives Matter to the New Black Panthers.

Simultaneously, the Al Qaida plotters are completing their preparations for massive improvised explosive device attacks. One plans to breach a dam in north Texas releasing the equivalent of 125 times the water released in the Johnstown Flood into small towns north of Dallas with a population of 431,000. Another is targeting the St. Louis Convention Center with a truck bomb set to go off during a Christian chorale convention. Both plots involve purchases of ammonium nitrate which is then delivered to private homes, most of which are abandoned or at least empty during the day so the bags of ammonium nitrate can be stolen.

Key Insights from the Simulations

General Insights

1. Influencing and shaping Gray Zone activities by states and non-state actors presents the United States with particularly difficult challenges, quite different in scope and impact from conventional warfighting. It may not be possible to influence or shape Gray Zone activities by other states or non-state actors, especially when those actions are not directed toward the United States.

In the IR-SA simulations participants struggled to shape the Gray Zone activities of the state actors because, while those actions may have had some effect on U.S. interests, the actions were most often not directed toward the U.S. Participants considered creative actions and reactions both inside and outside of the Gray Zone but sometimes found that the best available option was to take no action except to prepare for secondary or tertiary effects that might threaten the U.S.

2. Violent extremist organizations may act in the Gray Zone in an attempt to drag state actors out of the Gray Zone. State actors need to have appropriate strategies developed and responses queued for rapid delivery.

In an action drawn straight from the classic insurgency model, a non-state actor (VEO) urged followers to violence in the hope that over reaction by the state might in turn incite others to violence. Participants noted the VEO messaging but failed to act to counter it. So when adherents to the VEO ideology committed acts of violence, both the state and individuals acting independently of the state reacted, beginning a round of tit-for-tat acts of violence.

3. To operate effectively in the Gray Zone, U.S. policy designers and operators need a full quiver; a whole-of-government approach is crucial to success. In fact, we should begin to think in terms of a *whole-of-government-plus* structure where government reaches out to non-government regional and technical specialists, subject matter experts, and other "different thinkers" to formulate courses of action.

Throughout these simulations Blue missed opportunities to fully assess the significance of events, shape outcomes, or reduce tensions because, controllers felt, of the lack of specific subject matter expertise in areas like international finance and economics, law of the sea and the laws of war, refugees and migration, and religious sectarianism. Expertise in all of these fields exists in the national security enterprise, and profiting from this expertise by adopting country team or whole-of-government approach seems crucial to success in the Gray Zone.

4. The U.S. is not the sole major power assessing threats and opportunities in Gray Zone conflicts and competitions. It is possible that actions by other major powers could draw the U.S. further into conflicts or drive parties to violence.

Whether acting in concert with or independent of participants, other major powers can be expected to engage in activities that advance their own interests, not ours. During the two IR-SA simulations, Russia and China engaged in Gray Zone actions that conflicted with U.S. Interests, heightening tensions and frustrating U.S. strategies.

5. Controllers noted a clear bias among the U.S. government participants toward Saudi Arabia and against Iran, and a willingness to move directly to kinetic or other military action by some of the military players. Such overt biases and tendencies may adversely affect the ability of the U.S. to take advantage of opportunities for influence in Gray Zone conflicts.

It's hard to break old habits. A career spent observing Iran's belligerence toward America, its support for terrorism, and its antagonistic world view may have permanently shaped attitudes among those participants.

Additional Insights from the IR-SA Scenarios

Among the tasks given to ICONS by USSOCOM was to explore the capabilities needed for maneuver in the Gray Zone and how best to coordinate those capabilities. One participant offered that there is a need for "*the right cognitive abilities. Meaning, do we have the appropriate personnel in place who have the ability to look across the wide spectrum of destabilization and can assess (specifically from the strategic level) probability sets of reactive responses..?*" Putting the "*right type of personnel*" in place "*would be the sharpest tool we could have.*" Another noted that coordination of knowledge and information is as important as coordination of action, "*Important to have intelligence, diplomatic, and military all joined up.*

They each have to be in good communication with each other."One participant felt the U.S. government is not properly structured for operations in the Gray Zone: "*U.S. lacks a cabinet level information entity… dedicated to 1) develop the U.S. narrative, 2) disseminate the U.S. narrative, 3) counter adversary misinformation and disinformation. [This] could be coordinated in the NSC or the principals committee.*"

Another participant suggested better coordination among government officials, academics, and outside of government subject matter experts: "*What may be lacking in some instances, however, is fine-grained knowledge about the internal political and social dynamics of some countries ... This deficiency may blunt the impact of USG efforts to ease tensions, reassure allies, respond to threats, and so on, and in some cases may lead to USG responses that are indeed counterproductive. …The USG would benefit from reliable and up-to-date data on the social and political attitudes of ordinary citizens; an understanding of how these perceptions impact communal relations, political behavior, and orientations toward the United States; and an understanding of how these attitudes and behaviors relate to divisions within GCC ruling families. The USG can make use of these tools through engagement with scholars of Middle East politics and political economy. The participation of such individuals in the simulation, myself included, is an encouraging sign that such engagement is already ongoing. This simulation seemed to include a good balance of expertise across the military, diplomatic, and academic spheres.*"

Additional insights from the Foreign Fighters Scenario

The designers purposely created a challenging setting for this scenario in which participants who did not know one another were dropped into an ad hoc team with loosely defined roles and an intentionally dysfunctional communications system. We assumed that the two greatest challenges faced by the participants in this scenario were sharing information and the rapidity with which events occurred.

As we highlighted above, participants were asked to solve two rapidly evolving scenarios given patchy and sometimes conflicting data in order to stop two terrorist attacks. Information was provided to some teams and not others. Some of that information was fragmentary. Some of it led analysts and investigators down dead-ends. This was, the controllers felt, realistic. Communications and the sharing of information were the critical tasks to stopping the attacks.

The FLEA team players aggressively sought information with which to pursue their investigations. Following one large message release in which there was buried a note that more information was available upon request, the FLEA team disseminated relevant information around the other teams and sent in a request for additional information. In their team's conference room, members had already begun postulating theories and necessary responses. All this within seven minutes. This was indicative of play by the FLEA team throughout the simulation.

The Intel team faced an additional challenge in the scenario, but one that is both unique to the community and quite realistic outside the simulation: how to share highly classified information with clients and colleagues who do not possess top level security clearances (even though they may have a need to know). Inside their team conference, the Intel team worked through options and courses of action (including the use of tear line messages) all the while discussing the incidents in play and potential courses of action. Within the Intel conference controllers noted several times discussion of how to engage the other teams, especially the PAO team, to fully address the threat.

Inside that PAO conference, the participants' discussions covered the full range of media and public affairs issues including public statements by POTUS and others, the need to develop specific messaging directed toward to opposing sides of an explosive topic (gun control) following a terrorist

attack, and a decision to limit the amount of raw information forwarded to operators by synthesizing similar messages.

In addition to the intra-group messaging in conference, teams generated 143 inter-team messages, of which 101 were of substance (i.e., not simply a message forwarded, but a message with some value added comment by the sender). The messages included analysis of synthesized intelligence and media, requests for information, reports of actions taken by the National Guard or FBI, and so on. The FLEA team actually put the pieces together to solve the mysteries, but each team made it possible for that to happen.

It would have been easy for participants to miss one key piece of these puzzles and thus fail to solve these scenarios. In fact, both of the central attack scenarios presented pieces of critical data from three sources, with each piece given to only one group. Had any one of these pieces not been shared, evaluated, and processed, it was extremely unlikely that the task force would have stopped the terrorists from carrying out their attacks.

Some additional insights for this scenario included this from one participant: "*In the scenario as in real life, it is not easy to determine the boundaries and roles of organizations: what are the limits of the IC, what is known already to Law Enforcement and what cannot be shared*." Within the scenario participants were told that only members of the intelligence community team had clearance and need to know for information classified above the secret level. (NOTE: No actual classified information was used in this simulation.) Controllers then delivered to the IC reports nominally classified at the top secret level to challenge the team IC players to find ways to use the information they held without revealing sources or methods and so on. Members of the law enforcement team also received intelligence information from within federal, state, and local law enforcement intelligence channels.

Another participant noted that, "*The IC's ability to warn about a potential terror attack depends upon the amount and accuracy of the threat information we receive from the various intelligence channels*." We would take this to imply that analysts across the spectrum of intelligence and law enforcement need to share data, analysis, and hypotheses more broadly.

And, finally, another participant noted that the biggest challenge in the simulation was, "*Keeping up with the pace of the events, and developing a common operational picture*." Certainly this was a design feature of the simulation itself, but more broadly this is an important insight for the real world: things move quickly and it's hard to keep up.