



AMERICA'S NEVER-ENDING WAR

A WIKISTRAT CROWDSOURCED SIMULATION



September 2015



AMERICA'S NEVER-ENDING WAR

The new National Military Strategy of the United States warns that the Pentagon needs to prepare for a war with no end as the country faces new threats from violent non-state actors that appear to be advancing quicker than the U.S.'s ability to respond. Further complicating the threat environment is the rise of hybrid conflicts, where state and non-state actors are working together, posing enormous challenges to the nature of U.S. and allied responses.

To address these issues, Wikistrat ran an online, crowdsourced simulation in August 2015 involving more than 70 experts, who analyzed the threats and implications of a never-ending war over the next 25 years. This report contains some of the key insights Wikistrat's analysts generated.

THE U.S. SHOULD PREPARE FOR A NEVER-ENDING WAR – BUT AGAINST WHOM?

Islamic extremists in Africa

While most attention over the past decade has been on the war on terror in the Middle East and Afghanistan, our analysts highlighted Africa as a prime future target for terrorist groups. Porous borders, weak governance and corruption in the continent present ISIS with the opportunity to expand their terror and criminal operations far beyond Libya. Given the size of the African continent, it will be difficult for the U.S. to counteract any attempts by ISIS in Libya to expand if the organization gains a foothold. Consolidation of ties and greater cooperation between militants across Africa, both existing (e.g., Boko Haram or militants in the Sinai Peninsula) and potential (e.g., Al-Shabab), would bring further destabilization to key choke points such as the Suez Canal. ISIS may leverage its financial clout to acquire arms like anti-ship missiles and weapons systems, which they could use against Western military and civilian targets.

Exploiting the porous **West African** borders, Boko Haram will begin to play out ISIS scripts, attracting foreign fighters to target Western interests, including the United States. With the influx of skilled men and weapons, Boko Haram may become more violent, increasing its biological and technological warfare capabilities. For Boko Haram, forging closer links with ISIS and other Islamist groups is an important step towards gaining external legitimacy, funding and weapons. This would increase its capacity to spread destabilizing violence involving Cameroon, Chad, Niger, Nigeria and even Mali. Whether acting on its own or in collaboration with other groups, Boko Haram may use suicide bombers and armed attacks on U.S. diplomatic facilities and personnel, on U.S. business headquarters and on U.S. transportation and energy production sites.

ABOUT US

Wikistrat is the world's first crowdsourced consultancy. It leverages a global network of subject-matter experts via a patent-pending "Collaborative Competition" methodology to provide a variety of analytic services. Scenario generation, policy planning, risk assessment and red-teaming exercises are conducted by Wikistrat on a real-time, interactive online platform.

States employing others to do the fighting for them

One trend our analysts expect to increase and have a strong impact is that of states using non-state actors to do their fighting for them. As seen in Ukraine, **Russia's strategy of hybrid warfare** is likely to be long-lasting and will draw in not only Russians, but other pro-Russian foreigners from the former Soviet space. **Kazakhstan** may suffer a similar fate as Ukraine under a sudden and difficult regime change, with its northern Russian-majority regions being drawn into Russia's fold via violent separatists and masked "little green men." This becomes the trend in regional warfare and conflict, with **Georgia** also being particularly vulnerable to such intervention. In these scenarios, Russia will serve as a transit for volunteers seeking to fight on behalf of pro-Russian separatist forces in the region.

Cyberattacks by foreign criminal groups to steal information from U.S. businesses, the U.S. government or military targets **will increase** with the support and guidance of America's adversaries, such as China, Russia, Iran or North Korea. Military equipment (e.g., drones) will be hacked in real time, air traffic control and other critical infrastructure could be disrupted, and emergency responders may see their communications manipulated or severed. The use of criminal organizations here provides foreign governments a buffer of deniability in their attempts to obtain information on U.S. businesses or the military.

The **international private military industry** has expanded substantially over the past 20 years. Private security contractors (PSCs) have taken over functions traditionally carried out by governments, national militaries and international organizations. As more countries – especially major rival military powers like China and Russia – start to endorse PSCs, there will be more supply and demand for their services, ranging from logistics and management to force support and combat. Non-Western countries and companies seeking a non-Western PSC will have an alternative market. A primary threat here is that state-hired PSCs will be employed to support military operations against the United States. A secondary threat raised by the global increase of PSCs is more war worldwide. PSCs lower the barriers to war because they can offer high-quality, flexible services at relatively low cost, and allow governments to get involved in a conflict without using national military resources.

Enemies from within

Internal threats to the American homeland are likely to increase, say our experts, exacerbated by rising social divisions and the challenges of reintegrating military veterans. Since 9/11, **right-wing extremists** have been almost twice as deadly on American soil as jihadists. *New America* reported that, excluding 9/11 and the recent Tennessee shooting, jihadists have killed 26 people while right-wing extremists have killed 48. Because military veterans have desirable skills in weapons use, explosives and operating in dangerous environments, they will be targeted for recruitment by right-wing groups wishing to conduct attacks on civilian or military targets.

These returning veterans may be susceptible to recruitment if they feel a sense of disenfranchisement after leaving the military. The number of military-trained, right-wing extremists tempted to commit an act of terrorism is likely to be low, but the group is significant because of their deadly potential.

The U.S. military, after more than a decade of fighting in the global war on terror, has become the target of **lone wolf terrorist** attacks on domestic soil. While these attacks to date have been devoid of association with known terrorist organizations, radicalized individuals are often inspired by terrorist groups overseas that actively call for lone wolf attacks on military personnel within the United States.

WHAT CAN THE U.S. DO?

Invest in alliances

Effective **isolation and containment** of groups like ISIS demands a multi-layered, trans-border strategy that reflects the geographical context and the nature of the enemy, with an emphasis on strengthening the defensive capabilities of relevant institutions in the Middle East and North Africa. All branches of the U.S. military will be required to work closely with allies and local governments to strengthen local and regional capabilities. A key task for special operations forces (SOF) and Army personnel will be to help train Nigerian soldiers in their fight against Boko Haram.

Walking the walk – a more aggressive and proactive approach

Another option to counter the rising threat from ISIS and the perception that the U.S. is losing the global war on terror is for Washington to take a **more aggressive approach** towards removing and destroying the group. This will involve formulating and implementing a more robust military strategy for a regionally led and Islamic response with ground forces, as well as a more robust U.S. reaction in terms of frequency and scope of air and naval operations in Iraq, Syria and Libya.

Such an approach will also incorporate targeted use of SOF for surgical strikes against ISIS command and control assets. Further, it will incorporate those tools into a broader approach that challenges ISIS rhetoric in Islamic terms, with assistance from Muslim political and religious leaders in the heart of the Middle East.

To tackle the threats from **Russian proxies**, the U.S. needs to take a **more proactive approach**, including the following three key steps: identifying foreign fighters and mapping their transit to vulnerable countries, assisting governments in consolidating control over the official demarcated state borders, and planning response mechanisms for future flashpoints.

The very nature of PSCs limits the policy options open to the U.S. in countering potential threats. An important step will be for the U.S. government to support the enlargement and implementation of the **Montreux Document**, particularly to non-member countries.

No need for boots on the ground, but rather eyes and ears

As maintaining a large force presence overseas will remain politically and economically difficult for the U.S., a **robust command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capability** should be maintained even as force postures are drawn down in the region and militaries downsized. In regions where there is continuous conflict combined with poor and degraded infrastructure, there must be assets that can both collect information as well as help the U.S. and the West respond more efficiently to these and other threats.

DISCLAIMER

This report is for informational purposes only and does not constitute financial, investment, economic, financial planning, trading or any other advice. You should consult with a competent independent financial advisor before making any investment or other decisions and should independently verify information on which you rely. The report is provided without any express or implied warranty of any kind including warranties of accuracy, completeness, or fitness for any particular purpose. Without limitation, although we have prepared this report based on sources we believe to be reliable, legally derived, and unbiased, we can provide no assurance with respect to the objectivity or any other aspect of its content. In addition and without limitation, this report may contain predictions, estimates or other information that might be considered forward-looking or predictive. Such statements are subject to risks and uncertainties that could cause actual results to differ materially. We assume no obligation to update the report or any part thereof or to correct any inaccurate or outdated information and reserve the right to remove or modify the report, in each case without notice to you or any other party. Without limitation, this report is subject to the Terms of Service posted on our internet website at www.wikistrat.com.

ATTRIBUTIONS

[cover] This work, "cover", is a derivative of "Pararescue Training Exercise" by Petty Officer 2nd Class Scott Taylor, released into the public domain; "Joint Colors" by CrimsonScholar, released into the public domain; "Ramadi August 2006 Patrol" by Air Force Tech. Sgt. Jeremy T. Lock, released into the public domain; "USS America (LHA-6) off Pascagoula in 2013" by Senior Chief Aviation Ordnanceman Lawrence Grove, released into the public domain; "F-16 fighting falcon" by US Air Force/ Staff Sgt. Christopher Boitz, released into the public domain; "United States of America Flag at Half-mast in New England in Summer 2015" by Adam S. Keck, licensed under the Creative Commons Attribution-Share Alike 4.0 International license.

AMERICA'S NEVER-ENDING WAR

Author:

Air Vice-Marshal (Ret.) Steve Chisnall

Editors:

Eva Dubinsky and Steve Keller



September 2015