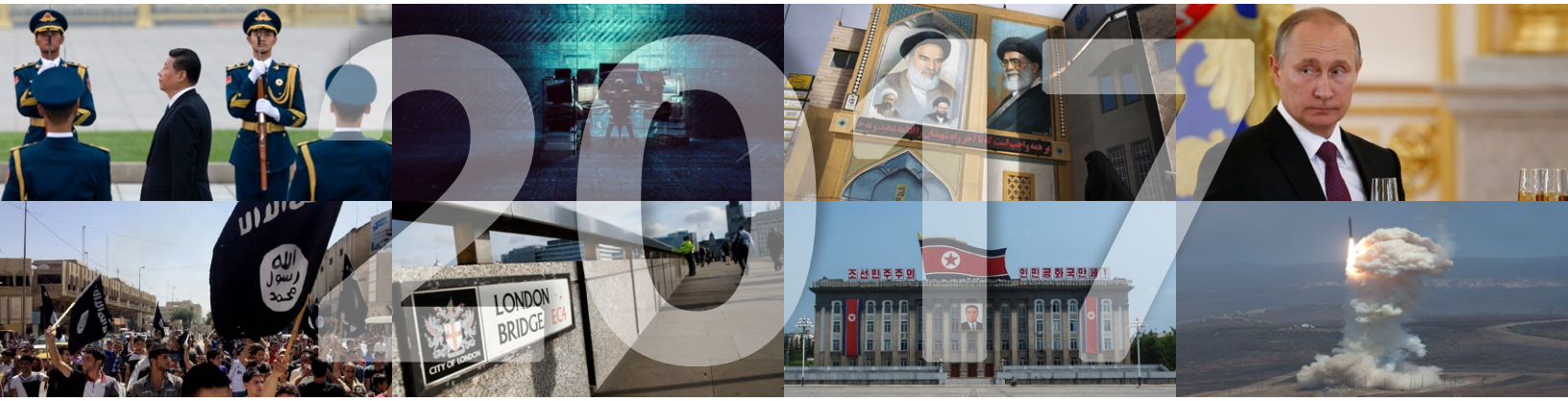
THE CIPHER BRIEF
ANNUAL THREAT REPORT



The world may have been more dangerous in the past, but our experts tell us it has never been more complicated.

THE CIPHER BRIEF

Letter from the CEO

Hello,

Thank you for downloading ***The Cipher Brief Annual Threat Report***.

I launched The Cipher Brief in 2015, after spending a career as a journalist, which included working as an international news anchor, an Intelligence Correspondent for a global news network, and an author. While I enjoyed the mainstream network news mission of telling the public what happened, I wanted more time to focus on talking about what the news events of the day actually meant to them.

I always knew, as most journalists do, that sources are a key part of understanding a story. To be blunt, the quality of sourcing across various news platforms today is varied, which makes it difficult to know how good the information that you're getting is. Who you choose as your source of information is critical to how you think about the context of global events. That's why I built The Cipher Brief with sourcing in mind. Many of the people we tap for insight have led intelligence agencies. Many of them have spent their careers undercover in dangerous parts of the world. They all share their insights and expertise on thecipherbrief.com.

We are truly unique in the market, with more than 75 proven national security expert contributors and more than 900 global contributors. We curate incredibly high-level thinking in combination with on-the-ground perspectives on events, and pull it together for our readers in an easily-digestible format. We tell you where the experts agree, where they disagree, and the likely path ahead.

This report is based on the extensive daily reporting and analysis that The Cipher Brief produces and publishes on our website, as well as the specific polling of experts we conduct on security issues.

We are a strictly non-partisan media company, which means we do not take political sides in thinking about security issues. In the daily content we produce on our website, we focus on innovation and on the critical contributions that the private sector makes to the overall global security picture. In short, whether in our reports or on our website, we produce content that focuses on harnessing the smartest thinking on the issues, not on the politics of the day.

If you'd like to learn more about The Cipher Brief, you can find a detailed list of our offerings at the end of this report. You can also sign up, for a limited-time, for a free subscription to our daily newsletter.

We hope you find this report easy to digest and useful in terms of understanding the complex, global security world rapidly unfolding before us and we'd love to include you in our future thought leadership-driven events. For more information on that, please email us at feedback@thecipherbrief.com.

Thank you,

Suzanne
CEO & Publisher
The Cipher Brief

The Cipher Brief polled its Network of more than 70 national security experts on what they view as the top 5 threats in the coming year – and why.

1. China
2. Russia
3. Terrorism
4. Nuclear Aspirants – North Korea and Iran
5. Cybersecurity

China

Xi Jinping: The Most Powerful Leader Since Mao?
Nationalist fervor, a more aggressive military posture, and curbs on free speech in China today are the hallmarks of one man: President Xi Jinping.

Source: AP Images

Our Experts Agree:

Chinese President Xi Jinping's consolidation of power, combined with China's growing wealth and global influence, affords Beijing an advantageous negotiating position on the world stage. But, with Xi's greater standing and influence over Chinese policy, he will be held responsible not only for China's successes - but also its failures.

- Rather than expand consensus and transparency, Xi has sought to draw more and more power into China's Communist Party, and specifically, into his role as leader of it.
- His rationale is that strong leadership is necessary for China to weather the existential problems it now faces.

China's behavior in the South and East China Seas is troubling, but here to stay. Much like North Korea's nuclear weapons, our experts feel that it is too late to change the state of play of Chinese militarization of islands in the South China Sea – instead, the only pathway that remains is to convince Beijing to adhere to international norms, such as Freedom of Navigation.

- While China is not the only country reclaiming land in the South China Sea Vietnam and Taiwan do the same—the scale and resources that only China can bring to bear make others in the region nervous.

Our Experts Disagree:

Over whether China can step into the global leadership role alongside – or in place of – the United States. China, despite its public acts of largesse, is managing multiple demographic, economic and political challenges, each of which is further complicated by centralized control by the CCP. So, despite fears of China "filling the vacuum" ostensibly left by the United States' recent withdrawal from international agreements such as the Paris Climate Accord or the Trans-Pacific Partnership, it is unclear whether the PRC will be able to do so.

- China's political stability is tied, inextricably, to its economic success, which has suffered not only a slowdown but also the effects of centralized mismanagement by the CCP.

- Major projects and investments are subject to the whims of Beijing's inside-baseball politics. As a result, China's political and economic risks are actually rising.

Move It Forward:

The U.S. must address the forgotten "pivot to Asia" of the Obama Administration and endorse, replace, revise – or terminate it. Our experts tell us that treating China as an afterthought – after terrorism or North Korea, for example – is a dangerous game to play. Rather, U.S. actions must be part of a larger, holistic strategy to address a rising China not only in East Asia, but around the world.

The U.S. must decide if it will compete with China on the world stage on global issues such as climate change, clean energy, free trade, and freedom of navigation. Each of these issues will determine the approach to sub- issues such the South China Sea.

- In the South China Sea, the U.S. cannot rely on Freedom of Navigation Operations (FONOPs) alone. When used as a "singular messaging tool," FONOPs can confuse other countries about Washington's intent.
- As Admiral Jonathan Greenert, former Chief of Naval Operations for the U.S. Navy, told The Cipher Brief, "FONOPs should be a tool in a regional tool bag, but not the only tool in the regional tool bag. When that happens, the program's purpose and intent become corrupted," and creates a misperception that freedom of navigation may be negotiable.

U.S. – China relations require delicacy and firmness all at once. It also requires leaders who can deliver on negotiated terms. Xi Jinping has clearly established himself as a power center in China, but has President Donald Trump?

Where Does the Administration Stand?

At their first meeting in April, Trump and Xi discussed trade and cooperation on North Korea, but sidestepped several other issues important to the bilateral relationship, such as tensions in the South China Sea and climate change. The summit was short on deliverables—with the only one being a 100-day plan to find ways to reduce the U.S. trade deficit to China—but served as an important personal introduction between the world's two most powerful heads of state and a reversal in Trump's attitude on China. In the weeks after the summit, Trump voiced his praise of Xi as a leader and reversed his decision to label China a currency manipulator, and the two leaders had several phone calls over managing tensions with North Korea.

Source: AP Images

However, it would appear recent events have eroded the good will fostered at the summit. Beijing's reluctance to increase pressure on North Korea and U.S. actions—sanctions targeting Chinese firms with ties to North Korea, two Freedom of Navigation Operations, and a $1.3 billion arms sale to Taiwan—have put the two nations back where they started, or perhaps in an even worse position.

Our Experts on China

"If we don't get this right, nothing else matters."

– General Michael Hayden, Former Director, CIA and NSA

"Xi has now identified his interests as the same as the Party's and the Party's as the same as China's. Therefore, the People's Republic of China will, in all likelihood, rise or fall with him."

– Gordon Chang, Author, ***The Coming Collapse of China***

"In my opinion, it is too late to reverse or undo occupancy [in the South China Sea], without risking a conflict. Our future strategy should assume these facilities are in place and active, and pursue limiting their use."

– ADM Jonathan Greenert, Former Chief of Naval Operations

Source: The White House Flickr

Russia

"Russian leaders, and Putin is no exception, respect strength and conviction…as history has illustrated, Kremlin aggressiveness can be checked when confronted with unshakable resolve."

– Michael Sulick, Former Director of the Clandestine Service, CIA

Our Experts Agree:

Russian President Vladimir Putin has framed himself as the leader of a global anti-U.S. movement, and seeks to return Russia to the status of a global power, with the according prestige and respect. Russia remains an existential threat to the U.S. – an adversary state with nuclear weapons.

- Putin will continually act to change the post-WWII global order and the structures that support it, such as NATO. This comes at a time when European unity is already in a fragile state.
- While Putin will attempt to counter the U.S. at every opportunity, it is unlikely he would do so in such a dramatic a way that it would demand open response. Aggression on the periphery – Ukraine, Syria, cyberspace – will likely continue.

But Russian success has its limits. Moscow's foreign adventurism may be flashy, but the domestic challenges Putin faces are grim; troubles at home partially explain Russian posturing abroad.

Our Experts Disagree:

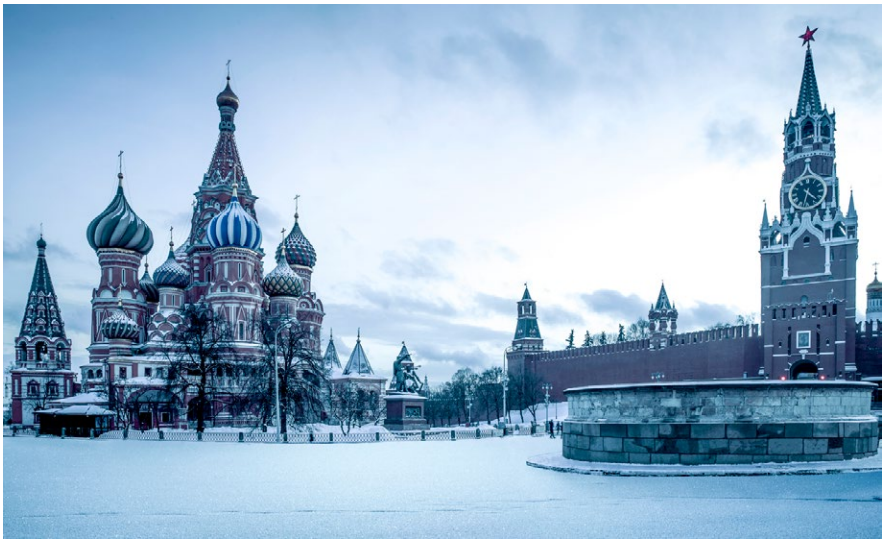
Over what 'standing up to Putin' looks like. Suggested policy paths range from strengthening allies and partners around the world to hardening cyber defenses to confronting Putin. All options require close coordination from Congress, the White House, and U.S. allies and partners; agreement which is not currently happening.

Source: AP Images

- The U.S. placed missile defense structures in multiple countries in Eastern Europe and deployed troops to Poland.
- The Trump Administration says it will continue to call out Russia for its support of Bashar al-Assad in Syria and actions in Ukraine. However, how the statements of Secretaries of State Rex Tillerson and John Kerry or UN Ambassadors Nikki Haley and Samantha Power differ remains unclear, as does what U.S. actions will follow the statements of Tillerson and Haley.

Move It Forward:

Don't count on détente anytime soon. The way ahead will likely consist of increased sanctions and "unshakeable resolve." Short of surrendering to Putin's view of the world, no U.S. Administration is likely to meaningfully change Russian behavior, particularly given Moscow's recent successes.



Source: iStock

However, sanctions have power: having witnessed the color revolutions in Russia's near abroad, Putin understands that his hold on power is subject to threat, should the Russian economy fail. Domestic public protests in recent months, triggered by government corruption and a weakened economy, strike fear in the Putin government. Mike Sulick, Cipher Brief Expert and former Director of the National Clandestine Service told The Cipher Brief, "despite Russian interference in U.S. elections, overall, Putin's policies have backfired -- and he may be more dangerous as a result."

Where Does the Administration Stand?

Questions remain over the Trump Administration's commitment to Article 5 of the NATO Treaty. Trump spent his first days in office calling NATO "obsolete" and pressing members to meet the two percent of GDP defense spending goal, or else. A few months in, Trump reversed course. At a news conference with NATO Secretary General Jens Stoltenberg in Washington in April, Trump called NATO "the bulwark of international peace and security."

- Still, at the NATO heads of state meeting in Brussels in May, Trump noticeably did not reaffirm America's commitment to Article 5, the bloc's collective defense clause, leaving many allies bewildered.
- Then, in a statement in the Rose Garden in June, he affirmed the U.S.' commitment to Article 5.

The Administration has struggled to put forward a comprehensive strategy to address Russian adventurism in the world, or even a response to the interference in the 2016 U.S. presidential election, an action that former Acting Director of the CIA Michael Morell told the Cipher Brief was "the political equivalent of 9/11." Trump policy, according to Former Vice Chief of Staff of the U.S. Army General Jack Keane, "has shifted from simply engagement and diplomacy to a willingness to confront. I think that is a major policy shift and one that is warranted."

- Though 17 U.S. intelligence agencies concluded unanimously, with high confidence, that the highest levels of the Russian government interfered with the American presidential election to delegitimize the U.S. electoral system, the White House has wavered on its support for this finding.
- In June, the U.S. Senate passed a sanctions bill that specifically included measures to prevent the White House from easing them; the bill is meeting resistance in the House of Representatives.

Russia's Election Interference

September 2015

The FBI informs a tech-support contractor at the Democratic National Committee that the organization may have been hacked. The contractor is unsure if the tip is real.


Source: iStock

June 15, 2016

American cybersecurity firm Crowdstrike releases statement naming the two entities responsible for hacking the DNC, Cozy Bear and Fancy Bear, as two "Russian intelligence-affiliated adversaries."

July 26, 2016

Intelligence officials from several agencies tell the White House they have "high confidence" that Russia hacked the DNC.


Source: iStock

October 7, 2016

ODNI and the Department of Homeland Security release a joint statement: "*The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the U.S. election process.*"

November 8, 2016

Donald Trump is elected President.

May 18, 2016

Then-Director of National Intelligence James Clapper says at a Bipartisan Policy Center event there are "some indications" of cyber attacks aimed at the presidential campaigns.

December 29, 2016

Obama expels 35 Russian diplomats and suspected intelligence operatives from the U.S. and imposes new sanctions targeting Russian intelligence services in retaliation for election interference.


Source: Elizabeth Cromwell

January 6, 2017

ODNI releases an unclassified report with a unified conclusion by the CIA, FBI, and NSA on Russian interference: "*We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.*" The agencies state "high confidence" in their judgements. Clapper, CIA director John Brennan, and FBI director James Comey brief Trump at Trump Tower on IC findings.

January 20, 2017

Donald Trump is sworn in as the 45th President of the United States.

February 13, 2017

National Security Advisor Michael Flynn resigns.

Source: AP/Carolyn Kaster

March 30, 2017

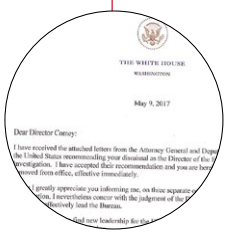
The Senate Intelligence Committee opens hearings to investigate Russia's interference in the election.

April 29, 2017

In a CBS interview airing on Trump's 100th day in office, Trump says "The concept of Russia with respect to us [the Trump campaign] is a total phony story." When asked if he believed the hack was phony, Trump responded "That I don't know," and later said "I'd love to find out what happened."

May 9, 2017

Trump fires FBI Director Comey, stating that the dismissal has nothing to do with Comey's role as lead investigator into Russia's intervention in the 2016 election.



THE WHITE HOUSE
WASHINGTON

May 9, 2017

Dear Director Comey:

Our Experts on Russia

"It is an attack on our very democracy. It's an attack on who we are as a people. A foreign government messing around in our elections is, I think, an existential threat to our way of life. To me, and this is to me not an overstatement, this is the political equivalent of 9/11."

– Michael Morell, Former Acting Director, CIA

"Still the only country that can destroy every major American city in a morning with a corrupt dictatorial leader whose strategic vision is restoring Russian influence and reducing American influence."

– John Bennett, Former Director of the Clandestine Service, CIA

"Russian leaders, and Putin is no exception, respect strength and conviction...as history has illustrated, Kremlin aggressiveness can be checked when confronted with unshakable resolve."

– Michael Sulick, Former Director of the Clandestine Service, CIA

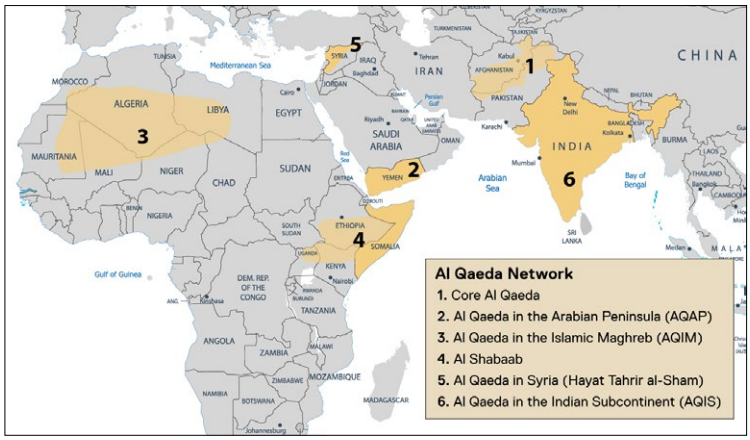
Source: AP Images

Terrorism: At Home and Abroad

"We cannot accept the current state as "the new normal." The American people will not accept it. We need to continue to disrupt and attack the threat as far from the homeland as possible while enlisting partner nations who have some creditability in the Muslim world to lead the messaging."

– John Bennett, Former Director of the Clandestine Service, CIA

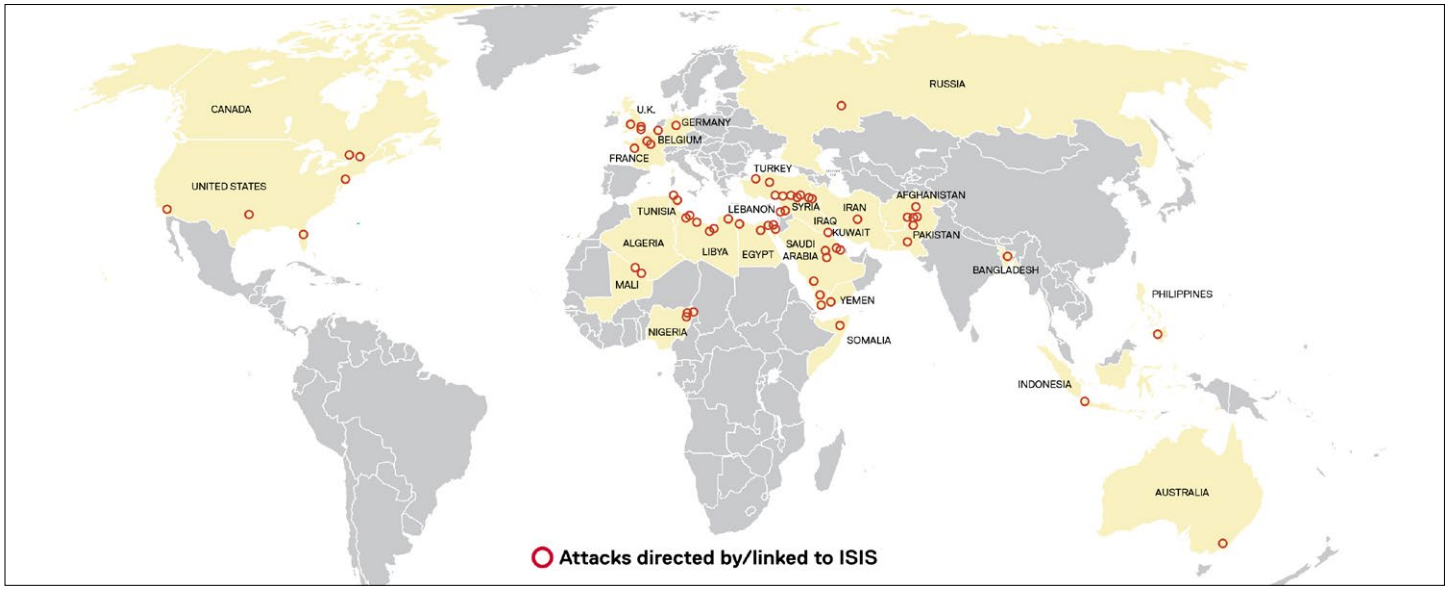
Our Experts Agree:



Removing terrorist groups' control of physical territory is a necessary, but not sufficient condition for defeating them. In the case of ISIS, the "caliphate" in Iraq and Syria is fundamental to the group's narrative. For al Qaeda and other terrorist organizations, ungoverned spaces in countries such as Afghanistan, Syria, Somalia, and Yemen provide safe havens where terrorist groups can recover, recruit, plan, and launch attacks globally. However:

- Resiliency is a primary military objective of terrorist groups. ISIS and al Qaeda have proven able to lose territory and subsequently morph into different, but equally dangerous, enemies.
- ISIS and al Qaeda affiliates have proliferated across the Middle East, South and Southeast Asia, Africa, and cyberspace.
- As terrorist groups come under increasing pressure on the physical battlefield, the threat of lone-wolf attacks inspired by online propaganda increases.

The West has failed not only to discredit the narratives and propaganda put forth by ISIS and other terrorist groups, but also, perhaps more importantly, to communicate a powerful 'big idea' that is more attractive to those susceptible to terrorist messaging. Terrorist groups, and ISIS in particular, exist both on and off the physical battlefield. Via cyberspace, ISIS has disseminated its message into the consciousness of populations around the world.

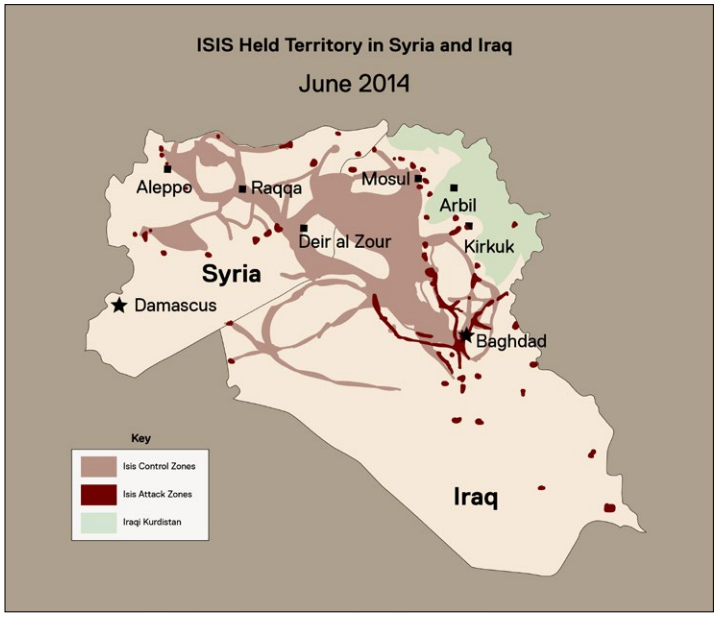


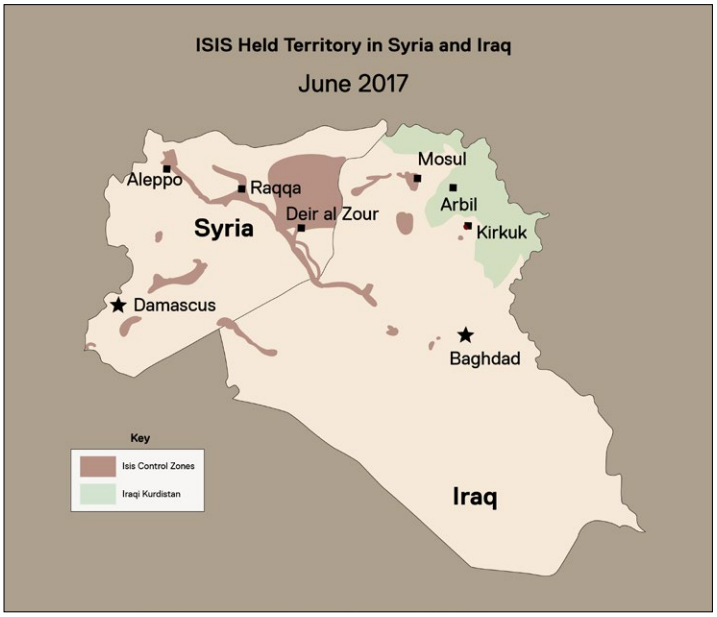
Our Experts Disagree:

On how to measure success in this fight. As ISIS loses its caliphate, it has spread to disparate locations around the globe because the fundamental drivers of its rise have not been addressed. A string of "tactical victories, but strategic defeats" has distracted from the larger question: is this fight about stopping terrorists or fixing the Middle East?

Despite agreement on the necessity to deny terrorist groups access to territory, there is no agreement on what comes next in Iraq and Syria or in Afghanistan. The "Day After" debate has found no answers, even after over 15 years of war.

- Some propose increasing support for good governance and credible power sharing agreements, as well as pan-Arab oversight of places such as Iraq, while establishing countering violent-extremism programs and community outreach in the West.
- Others propose a withdrawal from such problematic regions and an increase in use of airstrikes, surgical Special Operations Forces raids, and an end to "nation-building."





Move It Forward:

Solving the technology puzzle will be key, but again, not sufficient. Technology has transformed from a critical advantage for governments to a double-edged sword. As social media and encryption technology proliferate, they can serve as powerful messaging tools – or weapons – depending on who uses them.

Source: AP Images

- Terrorist groups' use of applications that obscure communications via end-to-end encryption will force governments around the world to either come to an agreement with technology companies to access that information or determine other ways to obtain the information.

- Counterterror and diplomatic efforts must better understand mass communication tools – social media among them – to effectively counter radical extremist messaging. But no technological solution will replace the need for a coherent, legitimate counter message.

Source: AP Images

Where Does the Administration Stand?

The Trump Administration's travel ban has been untested in counterterror efforts due to legal challenges preventing its enforcement; its existence, however, has been damaging in the counter-messaging campaign. One week into the Trump presidency, the Administration issued an executive order banning citizens from Iraq, Syria, Iran, Libya, Somalia, Sudan and Yemen from entry into the U.S. for 90 days. Protests at airports around the country and at the White House erupted; legal suits halted implementation. The Administration issued a second travel ban in early March, barring foreign nationals from the same countries – excluding Iraq – from entering the U.S. for 90 days. In late June, the Supreme Court allowed certain elements of the ban to enter into effect; the full case will be heard in the fall of 2017.

The Trump Administration has accelerated the war against ISIS in Syria, deploying several hundred Marines and Special Operations Forces to the country to support the Syrian Democratic Forces' assault on Raqqa.

- In response to a deadly chemical weapons attack launched by Syrian President Bashar al-Assad, Trump ordered a Tomahawk missile strike on the Shayat military air base, stating the retaliatory strike was "in [the] vital national security interest of the U.S.," and adding that "years of previous attempts at changing Assad's behavior have all failed."
- The strike on Shayat was an abrupt about-face for the Administration. A week before, White House Press Secretary Sean Spicer said the Administration "accepts the political reality" of Assad's rule.
- The strike was the most significant U.S. military action against Assad since the Syrian civil war started six years ago. But despite mixed statements from administration officials, there has been no word from Trump himself on what his ideal future for Syria looks like, or whether that future includes Assad.

Our Experts on Terrorism

"The region today is torn by no fewer than five dimensions of conflict: Persian vs. Arab; Shia vs. Sunni; democrats vs. authoritarians; terrorists vs. regimes; and terrorists vs. terrorists. Maneuvering through all of this requires unprecedented agility."

– John McLaughlin, Former Acting Director, CIA

"Even though the strength of al Qaeda and the Islamic State as standard bearers of the movement has waned in recent years, violent, militant Islam is spreading and deepening, globally...consequently, we can expect militant Islam to continue to grow as it morphs into new and violent forms."

– Rolf Mowatt-Larssen, Former Director of Intelligence and Counterintelligence, Department of Energy

"In the end, the scorecard is mixed: great tactical successes coupled with tragic strategic losses. We have won a lot of battles, but unless we shift course soon, we may lose the war."

– Kevin Hulbert, Former Chief of Station, CIA

Source: AP Images

Nuclear North Korea

"Two rather irascible, semi-cogent leaders facing each other down in very unpredictable ways. Mistakes are almost bound to happen."

– Michael Leiter, Former Director, National Counterterrorism Center

Our Experts Agree:

The North Korean nuclear threat is a threat of today, not tomorrow. Despite sanctions and international outcry, the pace of development in both missile and nuclear technology is only increasing. North Korea has deployed or is developing more than a dozen different missile types that vary in range, payload size, launch vehicle, and fuel type. Several of these have the range to strike South Korea and Japan, where the U.S. has tens of thousands of troops stationed.

China must play an equal, if not greater, role in managing the North Korean threat. China has long been a patron of the Kim regime in Pyongyang, and represents majority proportions of North Korean external trade, as well as oil and food supplies. The international community has long called on Beijing to exert greater pressure on North Korea.

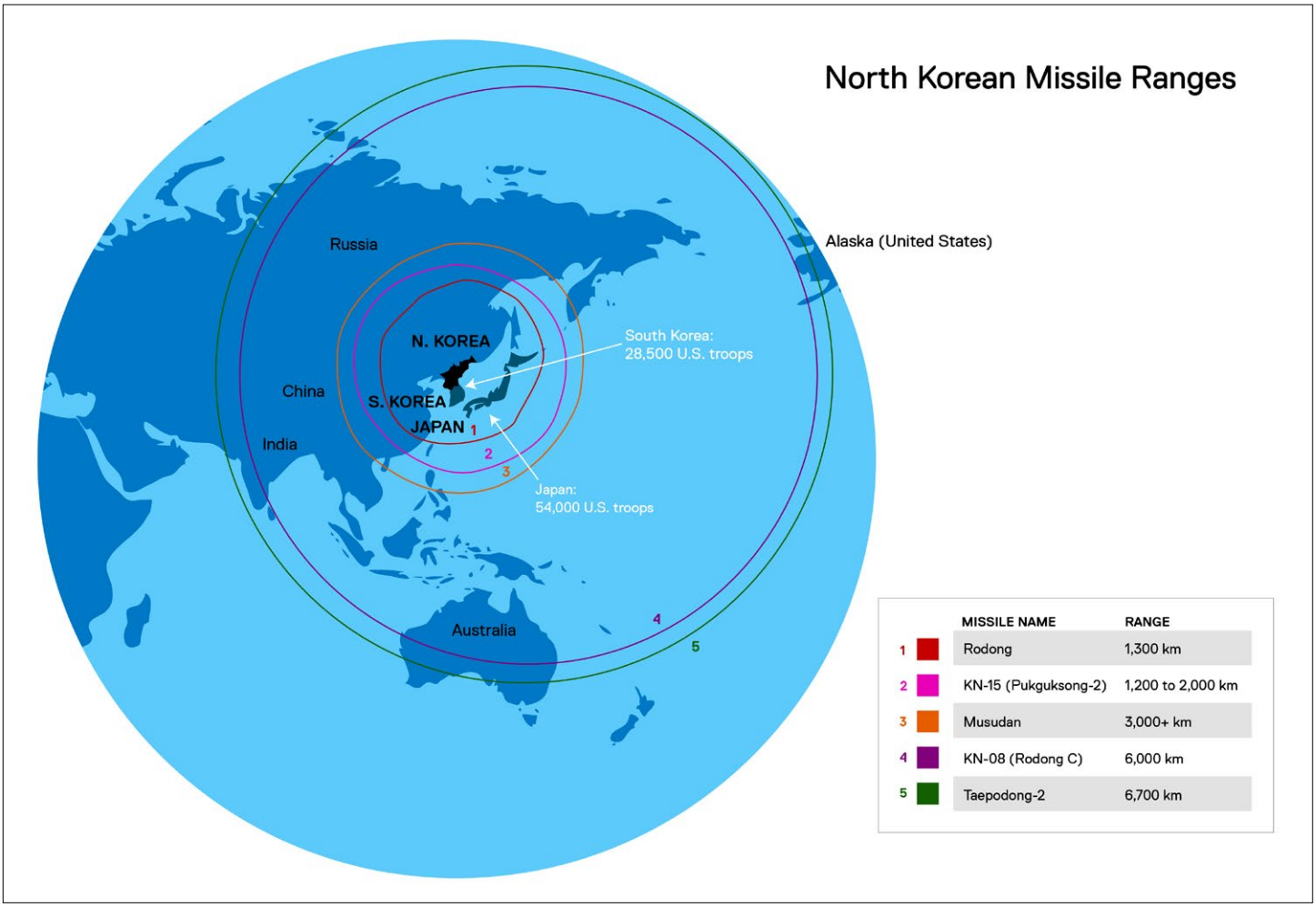
Our Experts Disagree:

On not only China's willingness – but more importantly its ability – to reign in the Kim regime. And, even if China is willing to cooperate, it is unclear whether Beijing has quite as much leverage as seems to be common wisdom.

On one side, our experts point out that China provides one key measure of support to Pyongyang beyond oil, food and other trade: Pyongyang acts with confidence that Beijing will remain its protector. North Korean leader Kim Jong-un relies on hardline elements in China's political system who have long ensured China's support of Pyongyang. Should this support appear to waver, or be used to exploit factionalism in the North Korean regime, China could wield greater influence than it does currently.

Source: iStock

On the other side, many note that China has real, strategic reasons to prevent action that hastens the fall of the Kim regime – and Kim knows it. Fears of massive refugee flows into the northeast provinces of China as well as the arrival of U.S. forces – supporting South Korean troops – on the Chinese border guide Beijing in all actions regarding North Korea.



Move It Forward:

The international community will not be able to denuclearize North Korea; it should instead focus on preventing North Korea from using the weapons it already has or proliferating nuclear technology. As Former Vice Chairman of the Joint Chiefs of Staff Admiral Sandy Winnefeld and Former Acting Director of the CIA Michael Morell told The Cipher Brief, "the first responsibility of a leader is to face reality. Setting aside our previous belief that we can convince North Korea to abandon its nuclear program will unlock the door to a different policy."

- The U.S. must reaffirm and demonstrate its support for South Korea and Japan.
- Sanctions – especially multilateral sanctions - should continue, if only to show commitment and deter other rogue nations seeking a nuclear weapon.

Time is a factor. Years of negotiations and sanctions have made little to no progress, and the Kim regime is under pressure. Recent purges by the young ruler as well as the assassination – allegedly ordered from Pyongyang – of Kim's older brother in Malaysia demonstrate instability in Kim Jong-un's rule that could drive increasingly provocative acts internationally.

- However, any negotiations must not be rushed to meet a political timeline.
- Negotiators should not trade items such as food, money or fuel in exchange for concessions the regime can easily renege on after delivery.

Where Does the Administration Stand?

Source: iStock

The Administration has strongly reassured regional allies Japan and South Korea that it takes the North Korean threat seriously. Since entering office, Trump repeatedly denounced North Korean provocations. Secretary of State Rex Tillerson, Secretary of Defense James Mattis, CIA Director Mike Pompeo and Vice President Mike Pence have traveled to the region.

- The Administration released a statement in April on its policy: "pressure North Korea into dismantling its nuclear, ballistic missile, and proliferation programs by tightening economic sanctions and pursuing diplomatic measures with our allies and regional partners," while leaving the option of negotiations open.

While Trump has expressed strong statements - that have exacerbated already high tensions with North Korea - much of Trump's stated policy is not new. "Tightening sanctions" and "diplomatic pressure" have been the hallmarks of previous policies toward North Korea.

- So far, remaining open to negotiations is the only major departure from Obama-era North Korea policy.
- According to Cipher Brief Expert and former Director of National Intelligence James Clapper, "the 'threat' has been profoundly and unnecessarily amplified by our own ill-advised rhetoric, which only serves to promote hyperventilation."

Nuclear Iran

"It is increasingly evident that the nuclear agreement with Iran has, at best, delayed but not dissuaded Tehran in its aspirations to develop a nuclear weapon."

– Mark Kelton, Former Deputy Director for Counterintelligence, CIA National Clandestine Service

Our Experts Agree:

Iran's strategic goals remain the same: expanding its influence in the Middle East, reducing U.S. clout and presence in the region, and countering Saudi Arabia and Israel. Because Iran's military capabilities and resources have been limited by years of sanctions, it relies on the Islamic Revolutionary Guard Corps (IRGC), proxies in Lebanon, Yemen, Iraq, Syria, and Bahrain, and cyber attacks to carry out its objectives.

Iran's pursuit of a nuclear weapon, though temporarily restrained by the Joint Comprehensive Plan of Action, is fundamentally tied to its larger aims to influence the Middle East. Iran's broader behavior and engagement with the world cannot be controlled by the JCPOA.

Our Experts Disagree:

Over whether the recent re-election of President Hassan Rouhani demonstrated an eagerness in Iran for reform and engagement with the West, which directly impacts the future of the nuclear deal. While there is no doubt that Ayatollah Khameini and the IRGC – the so-called "Guardians of Orthodoxy" – still firmly hold power in Iran, questions remain about the depth of polarization in Iran and whether there are credible moderates that should be supported.

Source: AP Images

The impact of the JCPOA and its chances of successfully preventing Iran from obtaining a nuclear weapon remain to be seen. The Office of the Director of National Intelligence's 2016 Worldwide Threat Assessment stated that "Iran does not face any insurmountable technical barriers to producing a nuclear weapon, making Iran's political will the central issue."

- On one side, our experts feel that the deal has failed to truly restrain Iran's pursuit of a nuclear weapon and has simultaneously freed billions of dollars that Tehran is using to dictate events in the Middle East. Many also feel that Iran cannot be trusted to adhere to the terms of the agreement.
- On the other side, proponents of the JCPOA point to the stringent international monitoring measures instituted by the deal, which create transparency and therefore minimize any attempts at cheating by Iran. Moreover, the money and sanctions relief were meant as carrots to bolster the "political will" necessary for Iran to move away from its pursuit of a nuclear weapon.

Move It Forward:

While there will be little change in Iran's behavior in the short-term, non-nuclear related sanctions should remain in place. The U.S. must remain willing to confront Iran for its support for terrorism and egregious human rights violations. Moreover, consideration should be given to identifying and supporting a moderate, democratic opposition in Tehran.

The U.S. must continue to back key partners in the region, such as Saudi Arabia and Israel. By showing a willingness to confront Iranian behavior, as well as bolster its partners, the U.S. can enable an alliance to counter Iran's influence in the region.

Where Does the Administration Stand?

Source: Getty Images

Despite "officially putting Iran on notice," the Trump Administration has retained the JCPOA. While on the campaign trail, then-presidential candidate Donald Trump stated that his "number-one priority is to dismantle the disastrous deal with Iran." Instead, President Trump has pledged to strictly enforce and monitor Iranian behavior relating to the agreement.

While the U.S. has maintained JCPOA-related sanctions relief for Iran, the U.S. Treasury Department enacted new sanctions on individuals and entities connected to Iran's ballistic missile program. In May, the Department of State issued a statement that the U.S. will "continue countering Iran's destabilizing activity in the region, whether it be supporting the Assad regime, backing terrorist organizations like Hezbollah, or supporting violent militias that undermine governments in Iraq and Yemen."

The Trump Administration sent a clear message to Iran during a visit to Saudi Arabia in May 2017. Not only did President Trump demonstrate a willingness to call out Iran for its behavior, but he also communicated support for the U.S.' Arab partners in the region. During his first trip overseas as President, Donald Trump delivered a speech at the Arab Islamic American Summit in Riyadh where he harshly criticized Iranian behavior in the Middle East, calling the Iranian government a leading state sponsor of terrorism.

Source: iStock

- In the speech, Trump noted that "from Lebanon to Iraq to Yemen, Iran funds, arms, and trains terrorists, militias, and other extremist groups that spread destruction and chaos across the region."
- According to Cipher Brief Expert General Jack Keane, "that was really quite extraordinary. No American President has ever spoken like that. Leaders in the Middle East and North Africa feel very strongly that the U.S. now has their back."

Our Experts on Aspiring Nuclear Powers

"[The Iran nuclear deal] is financing Iran's strategy and ambitions to dominate the Middle East."

– General Jack Keane, Former Vice Chief of Staff, U.S. Army

"The U.S. objective needs to shift from denuclearization to deterring [North Korea] from ever using or proliferating its nuclear weapons."

– ADM Sandy Winnefeld, Former Vice Chairman of the Joint Chiefs of Staff and Michael Morell, Former Acting Director, CIA

"Korea: Have to list it, but the "threat" has been profoundly and unnecessarily amplified by our own ill-advised rhetoric, which only serves to promote hyperventilation."

– James Clapper, Former Director of National Intelligence

Source: Missile Defense Agency

The Cyber Threat

"The new administration should learn an important lesson from all prior attempts to develop a comprehensive national cyber strategy: time is the enemy."

- Gilman Louie, Founder and Former CEO, In-Q-Tel

Our Experts Agree:

Vulnerability to cyberattacks by both nation-states and criminals cannot be solved without a paradigm shift in how governments, businesses and individuals share information and educate themselves about the security risks inherent in a technology-dependent world. Massive breaches and ransomware attacks, compromising the data of millions, will continue.

Source: iStock

Governments cannot solve this crisis alone. Government over-classification and industry concerns over proprietary information, however, have hindered information-sharing between the public and private sectors.

Technology is a double-edged sword and both sides are racing to find the next advantage. In the past, governments and established industry enjoyed a vast technological advantage. But, with the pervasive growth of internet access and ready-made cyber capabilities abundantly available, the barrier for entry into the virtual battlefield has never been lower. Even so, our experts agree that further innovation in technology will offer solutions for both government and the private sector.

Our Experts Disagree:

Over what comprises effective deterrence and response to attack in cyberspace. There seems to be strong agreement that governments and business need to raise the cost to attackers in cyberspace, but no consensus on what those actions look like – and whether they work.

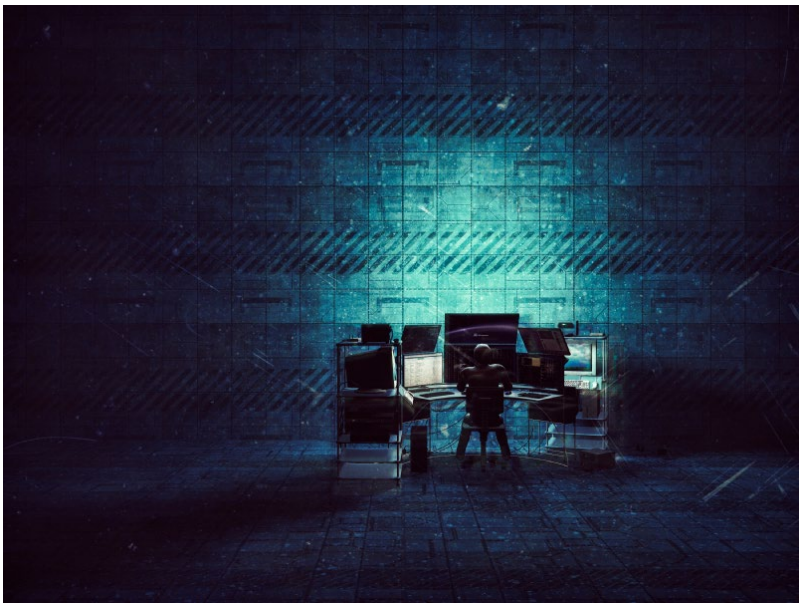
- A 2015 agreement – reinforced by the threat of sanctions - between then-President Barack Obama and Chinese President Xi Jinping seemed to limit Chinese economic espionage, but many believe Beijing simply moved on to other priorities, including military hacking.
- To date, the only public response to Russian hacking during the 2016 Presidential election has been economic sanctions. Multiple current and former U.S. intelligence and law enforcement officials have warned that Russian hacking will be back in 2018 and will, in the meantime, target elections in allied countries throughout Europe.

The stalemate between privacy and security remains an Achilles' Heel for both governments and industry. States are attempting to exert national sovereignty over cyberspace – to combat both criminals and emboldened adversary nation states - via controversial new laws. From battles over encryption technology to government disclosure of vulnerabilities, the rift between Washington, DC and Silicon Valley – represented in our experts' disagreements - limits the cooperation necessary to confront a common enemy.

Move It Forward:

The importance of public-private partnerships in solving cybersecurity issues will only increase. In this challenge, time is the enemy. Because time is a critical variable in protection against and response to cyberattack, information sharing between the public and private sectors must be as seamless as possible. The Cyber Threat Information Integration Center under the Office of the Director of National Intelligence could be given an expanded role similar to that of the National Counterterrorism Center to create a comprehensive understanding of cyber threats. The Department of Homeland Security's National Cybersecurity and Communications Integration Center can act as a necessary storefront between the nation's intelligence engine and the businesses that require pertinent and timely exchange of intelligence on cyber adversaries.

- In a conversation with The Cipher Brief's CEO and Publisher Suzanne Kelly, Rob Joyce, the White House cybersecurity coordinator and former head of the National Security Agency's elite Tailored Access Operations unit, highlighted the government's goals of securing federal networks and creating partnerships with industry so that malicious actors cannot hold U.S. critical infrastructure at risk.
- "We as the government have to be able to bring our capabilities to addressing the threats they are facing. We will know things that will inform companies on the threat, and must help them through process and regulation, and equip them with the tools the federal government brings," says Joyce.



Source: iStock

Hardening the defenses of key U.S. networks is critical, but so too is engagement with other countries. The United States has an opportunity to lead global efforts to refine and uphold conventions and standards – "rules of the road" so to speak – for cyber activity in the international order. Applying international norms to cyberspace, while difficult, will formalize and ease the development of proper deterrence and response policy.

Where Does the Administration Stand?

The long-anticipated Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure signed by President Trump in mid-May emphasized one key element: resilience. Described by our experts as "a plan for a plan" the order increased accountability of federal agencies regarding ensuring proper protection against cyberattacks, called on all agencies to use the National Institute of Standards and Technology framework, and ordered reports on multiple critical variables in cyber protection.

- According to Cipher Brief Expert James Lewis, "Like the references to risk management, resilience suggests an acceptance that we cannot now prevent cyber attacks, that we cannot keep attackers out, and instead must be prepared to deal with compromise and disruption when they inevitably occur."

Our Experts on Cybersecurity

"The Empowered Individual: What was once limited to technologically enabled nation states is now available to groups and individuals with whom traditional deterrence is ineffective."

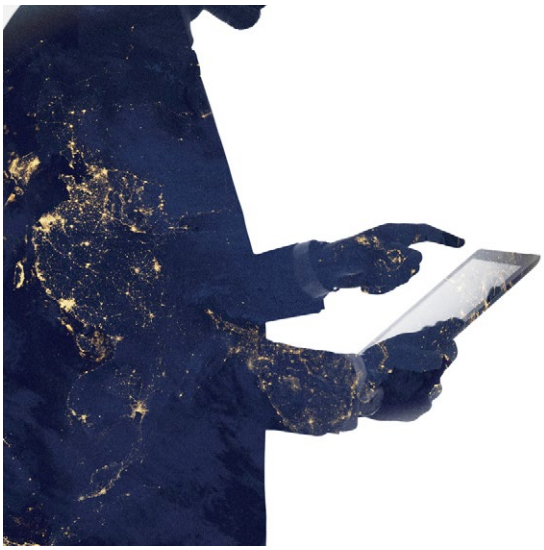
– General Stanley McChrystal, Former Commander, International Security Assistance Force

"General economic and technological trends...will help alleviate the challenge of encryption."

– Matthew Olsen, Former Director, National Counterterrorism Center

"The new administration should learn an important lesson from all prior attempts to develop a comprehensive national cyber strategy: time is the enemy."

– Gilman Louie, Founder and Former CEO, In-Q-Tel



Source: iStock

“The Worst of the Rest”

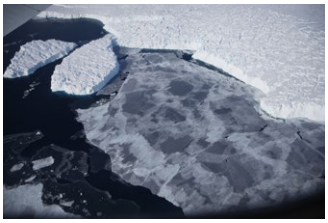
1. Pandemic

Source: Getty Images

2. European Implosion

Source: iStock

3. Climate Change



Source: Getty Images

4. Failed States and Ungoverned Space

Source: AP Images

5. Afghanistan

Source: iStock

6. Populism

Source: iStock

7. Demographic Change

Source: Getty Images

8. The Refugee Crisis

Source: Getty Images

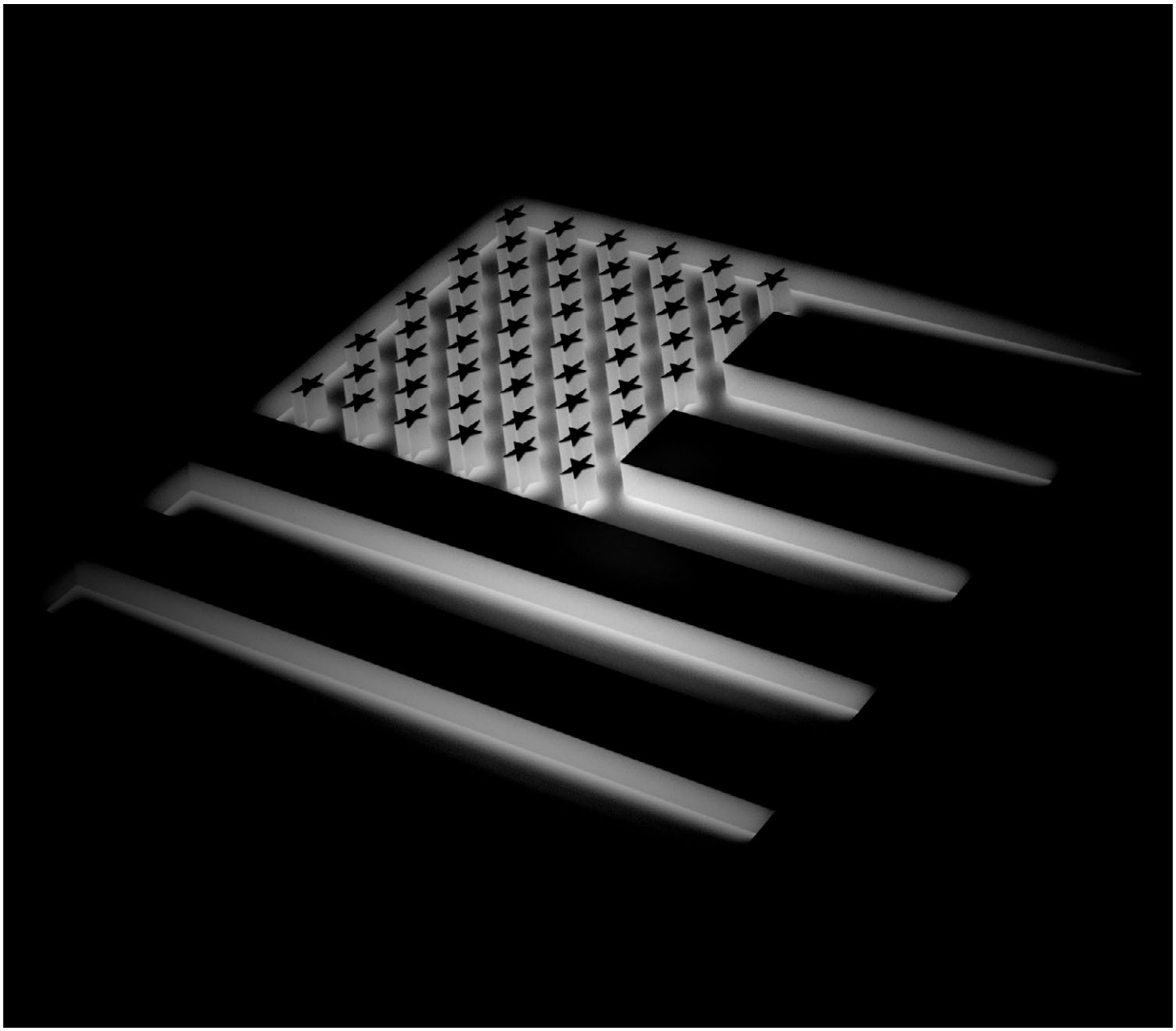
9. Economic Collapse

Source: Getty Images

10. Transnational Organized Crime

Source: Rodrigo Abd

An Unexpected Threat: Ourselves



Source: iStock

A Changing Global Order and a Distracted America

Many members of the Cipher Brief's Expert Network expressed that in addition to their "Top 5" threats, they also had great concern regarding the United States' ability to focus and react to a global crisis given its own internal divisions and domestic issues.

- Weakening of U.S. Alliances and Leadership
- A "Broken" Education System
- Executive and Legislative Branch Dysfunction
- A Drug Epidemic

> *"Internal Threat: Hugely damaging to our capabilities; unfortunately, we'll have more such losses."*
> – James Clapper, Former U.S. Director of National Intelligence

> *"Congress's inability to get out of its own way, along with politicians' prioritizing politics over patriotism, has tied the government's budgeting processes in knots."*
> – Admiral James 'Sandy' Winnefeld, Former Vice Chairman, Joint Chiefs of Staff

> *"America's internal polarization: Why? [It] diminishes the U.S. image as a model to emulate, and makes us less reliable as partners to combat a range of national security threats, thus emboldening adversaries."*
> – Michael Sulick, Former Director, CIA National Clandestine Service

> *"I believe our most enduring threat is "fake news" and the struggle over what is fake and what is not, which then breeds distrust in factual/real news. Over time we will have an increasingly uninformed electorate and it's also likely that this distrust in news overall will generate an apathy for the democratic process."*
> – Doug Wise, Former Deputy Director, Defense Intelligence Agency

> *"The post-WW II order with both US-led military and political/economic alliances has brought us greater wealth and security than any period in global history. The weakening/fracturing of institutions like the EU, NATO, as well as a lack of U.S. leadership on efforts like the TTP will provide our adversaries with opportunities that we will have trouble countering alone."*
> – Michael Leiter, Former Director, National Counterterrorism Center

> *"The End of Trust. Despite all its complaining, most governments relied on strong and reliable U.S. leadership in the world as a guarantor of the global system. The current administration's America First foreign policy and unconventional and unpredictable behavior will affect the decision making of other governments…A less trusting and predictable world is also a more dangerous one."*
> – Carmen Medina, Former CIA Deputy Director of Intelligence

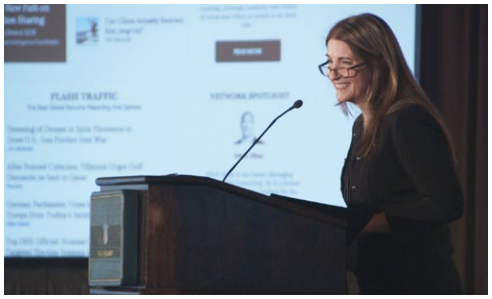
> *"We have a drug poisoning epidemic in this country, which doesn't get the focus it should. 129 people a day die of drug poisoning. One might contemplate that, in contrast to how people in the U.S. have been killed by terrorism."*
> – James Clapper, Former U.S. Director of National Intelligence

> *"Ayn Rand-think and strategic bankruptcy."*
> – James Lewis, Senior Vice President and Program Director, CSIS

Thank You

Thank you for your purchase of The Cipher Brief Annual Threat Report. The conversation about these threats continues daily on thecipherbrief.com with an expanding list of global experts.

For more information about **The 2018 Cipher Brief Annual Threat Conference**, an ***invite-only*** event, providing high-level engagement opportunities with Cipher Brief experts, please contact us at info@tcbconference.com.

For information about getting your company brand in front of The Cipher Brief's influential readership, via our digital platform, newsletters, podcasts or in-person briefings and events, please contact us at sponsorship@thecipherbrief.com.