Global Security Review

2017 Geopolitical Security Report

A review of the critical events & issues of 2017 that will shape the geopolitical landscape of 2018 and beyond.
Table of Contents

1. What is Hybrid Warfare?

2. Reconceptualizing Acts of Foreign Aggression

3. The Problem With Russia’s Nuclear Weapons Doctrine

4. Facebook, Compromised: How Russia Manipulated U.S. Voters

5. Cambridge Analytica: The Darker Side of Big Data

6. Russian FSB Official Linked to DNC Hack Charged with Treason for "Aiding CIA"

7. Trump’s Attempt to Co-Opt the National Security Agency has Backfired

8. Donald Trump Jr's Secret Communications with Wikileaks

9. The Subtext of Secretary Mattis' Mysterious Memo

10. Trump Campaign Officials Indicted in Special Counsel Investigation
11. Crisis in Venezuela: Economic Collapse, Violent Unrest, and Human Survival

12. How Likely is a Civil War in Venezuela?

13. Forget about North Korea, Venezuela is the next major national security crisis

14. China’s Economy on Unstable Ground: Debt Skyrockets as Unemployment Spreads

15. Saudi Corruption Crackdown Could Permanently Boost Oil Prices
What is Hybrid Warfare?

Contemporary U.S. and international legal framework governing acts of irregular and hybrid warfare severely impede effective de-escalation of and resolution to present hybrid conflicts.

Conventional Western (mainly American) concepts of war are incompatible and fundamentally misaligned with the realities of war in the twenty-first century. The emergence of a unipolar post-Cold War world order has resulted in a significant paradigm shift.

This change now requires the U.S. and its allies to adopt a new legal, psychological, and strategic understanding of warfare and use of force, particularly by state actors.

The term “hybrid war” (military institutions use the term “hybrid threat”) connotes the use of conventional military force supported by irregular and cyber warfare tactics. In practical application, the Russian concept of “nonlinear conflict” exemplifies hybrid warfare strategy.

Linear conflicts are defined by a sequential progression of a planned strategy by opposing sides, whereas nonlinear conflict is the simultaneous deployment of multiple, complementary military and non-military warfare tactics.

A nonlinear war is fought when a state employs conventional and irregular military forces in conjunction with psychological, economic, political, and cyber assaults. Confusion and disorder ensue when weaponized information exacerbates the perception of insecurity in the populace as political, social, and cultural identities are pitted against one another.

This “blurring” divides influential interest groups and powerful political organizations by exploiting identity politics and allegiances. Additionally,
nonlinear warfare tactics act as a deterrent towards a more powerful ally of the besieged state.

To use the Ukrainian conflict as an example, Russian tactics in the annexation of Crimea and the subsequent civil war in eastern Ukraine caught the West off guard (the U.S. and U.K., in particular) and unable to guarantee Ukraine’s sovereignty.

NATO’s in action can, at least, partially be attributed to the rigid military taxonomy presently employed to define warfare. More critically, Russian military and intelligence experts have accurately identified and exploited international legal frameworks governing the use of force against a sovereign state.

Take, for instance, the dichotomy that exists in the realm of international law between the concept of “war” and the idea of cyber conflict, electronic warfare, and information warfare. To date, there hasn’t been any measurable Western response to Russian hybrid aggression.

Unless the legal framework defining an act of aggression is reworked, liberal democracies are at risk. Presently, it seems increasingly clear that the primary means of ensuring the continued rule of law is by overhauling our traditional interpretation of conflict. The West must develop a framework of strategic deterrence of weaponized information, finance, and other subversive forms of aggression. A “one size fits all” policy would not be an effective deterrence.

U.S. military strategy above all must emphasize non-linear thinking in conflict modeling.

Rather, analysts should review each conflict independently. The degree with which states will employ non-military and active measures will vary significantly, as will the actual measures themselves.

Further, the flexible nature of hybrid warfare allows for more of a “trial-and-error” approach to foreign intervention, not unlike the agile development process used in marketing and technology firms. Russia’s continued Ukrainian escapades—exemplify the concept of agile warfare. The proliferation of such tactics allows for a much more efficient and less-costly forum to test the efficacy of proposed nonlinear tactics.
Developing a comprehensive suite of actor-specific offensive-defense or defense-through-guaranteed-aggression policies—underwritten by a demonstrated ability to launch a multilateral response—would serve as one measure to dissuade further aggression from irregular powers and rogue states.
Reconceptualizing Acts of Foreign Aggression

Adversarial powers like Russia view "active measures" in the West as integral to their military doctrine.

The current state of affairs between the U.S.-led West and Russia increasingly seems like a second "Cold war." However, this is a misstatement. Western institutions and social discourse have been caught almost entirely off-guard by the Kremlin’s strategic exploitation of our rigid military taxonomy. Russia has been unilaterally engaged in a nuanced war of contradictions and weaponized information. In short, Russia and the U.S. maintain fundamentally different definitions of the very concept of war.

The U.S. military has been undergoing restructuring based on its experience in Afghanistan and Iraq—against what it perceives as nonstate actors, insurgents. Meanwhile, a newly emboldened Russia flexes its' military power. How did this happen?

Failure to redefine conflict through nonlinear warfare tactics is a dangerous long-term strategy.

First and foremost, U.S. (and Western allies) must restructure both civilian and military elements of the national security apparatus. Accordingly, the core ideas of national security and warfare as legal, practical, and existential concepts that have been maintained by the West are no longer applicable. We must regard combat in an entirely new light—in the legal sense, in the definition of an "Act" of war, and in our understanding of civic responsibility in the digital age. Last, there exists the necessity to positively and inclusively engage the Russian youth.
The West must restructure its societal self-perception, which is far too vulnerable in its current state. Our failure to perceive cyber and traditional warfare as distinct entities is a prime example of a necessary shift. Failure to accurately conceptualize war is a danger to national security and risks destabilizing or utterly abolishing the rules-based, international order established in the wake of the USSR collapse.

Russian military planners recognize that, despite the considerable strategic and tactical nuclear arsenal, they have no effective means of waging a successful war or at least reaching some degree of conventional force parity with the U.S. and its Western allies. Conversely, U.S. leaders have struggled to conceptualize asymmetric measures of influence-projection, like Russia's concept of nonlinear warfare.

*Like an “agile” startup, with a perpetual “innovation-cycle:” Russian nonlinear tactics greatly benefit from the cycle of hypothesis establishment, experimentation, analysis, and iterative review to discern the most efficient way to producing disorder. Such chaos makes it difficult for dissenters both outside and inside the country to resist.*

Western military strategists over-rely on a rigid structure of categories or taxonomies in their effort to build a useful model for various types of conflict. Cyber operations have been treated as a distinct domain—a domain of lower strategic importance than warfare in the traditional sense.

In contrast—to the detriment of U.S. strategic interests—adversarial powers rely on a nuanced mixture of conventional arms, cyber warfare, and the dissemination of strategic communications through traditional and digital media outlets to deliberately sow confusion and dissent within a target territory or state.

### Non-Linear War is the New Form of Warfare

Termed by some “the Gerasimov doctrine”—following the publication of an
essay by Chief of the Russian General Staff Valeriy Gerasimov—this is a misnomer. The concept of “nonlinear” warfare has also been somewhat incorrectly referred to as “asymmetric” or “hybrid warfare.” The latter two originated following the NATO invasion of Afghanistan, and the U.S.-led coalition’s invasion of Iraq and the ensuing insurgency that arose.

Before the 2001 and 2003 invasions of Afghanistan and Iraq, the U.S. had limited experience in counter-insurgency and long-term combatant with non-state actors. The term “hybrid” or “asymmetric” warfare was used to define this new paradigm.

However, the system of classification has, yet again, proved to be the U.S.’s Achilles heel. Without a doubt, the United States possesses insurmountable conventional military strength and continues to pose an undoubtedly credible threat of mutually assured destruction through its strategic nuclear arsenal.

Both Russia and China realized early on that technological advancements in the fields of information technology and population (commonly termed market) research and analysis could be effectively weaponized and integrated into a multichannel offensive military strategy that would have far-reaching advantages when it came to confrontations with the less-agile, current policies pursued by U.S. military planners.

Moscow’s success stems from their “total” or "all-in" conception of war. A Sparta for the modern era, the Putin regime has been heavily investing in modernizing its outdated soviet-equipped military. This model depends on the blurring of lines between state and non-state actors, alliances and adversaries; even war and peace.

Starting in 2008, Russian special forces, financial tools, political subversion, information warfare, and other active measures launched a simultaneous and complementary assault on Georgian infrastructure. The Georgian state was paralyzed as a result and was unable to act, resulting in the de-facto secession of the territories of Abkhazia and South Ossetia.
Russian special forces in Crimea. Also called "little green men," they were one of the offensive "columns" that resulted in their annexation of Crimea from Ukraine.

A similar scenario occurred in Moscow’s annexation of Crimea from Ukraine in 2014, with their incredibly executed apparatus of plausible deniability using information warfare, insurgent funding, and economic warfare to utilize proxy “local actors” to achieve individual goals. Somewhat like an “agile” startup, with a perpetual “innovation-cycle:” Russian nonlinear tactics are strikingly similar to those employed by the marketing departments of silicon valley tech start-ups.

Somewhat like an “agile” startup, with a perpetual “innovation-cycle:” Russian nonlinear tactics are strikingly similar to those employed by the marketing departments of silicon valley tech start-ups.

The iterative cycle of hypothesis establishment, experimentation (a/b testing), analysis, and iterative review, repeated endlessly, has been the most efficient way of creating disorder. Such chaos makes it difficult for dissenters both outside and inside the country to effectively mobilize their compatriots, overloading social media and data streams with information and traffic from botnets and trolls.

Such chaos makes it difficult for dissenters both outside and inside the country to effectively mobilize their compatriots, overloading social media and data streams with information and traffic from botnets and trolls.
21st Century Military Planning Requires Nonlinear Thought

Linear thinking has long-dominated military planning. This concept depends on reliance on a state's self-interest above-all-else. In a linear thought model, one lays out a strategy through detailed planning, and established processes, step by step detail management tips, and customer service expectations.

Linear thinking has dominated Western military strategy until the end of the 20th century—only now are we beginning to realize the unprecedented threat we’ve been unknowingly facing. To combat Russian “active measures” like those currently being inflicted upon the democratic institutions and society of the United States, both civilian and government sectors at all levels can begin working on strategic plans for information security and compliance.

The ability to project force through a multitude of traditional and “nonlinear” mediums is tantamount to U.S. national security interests—particularly if they are utilized by a foreign adversary for subversionary tactics against the interests of the United States. Continued relativity when it comes to warfare is not an option in the 21st century. Western powers must recognize this new paradigm of war and adjust military doctrine accordingly.
Russia's military doctrine dictates the use of nuclear weapons in response to any non-nuclear assault on Russian territory.

Russia’s military doctrine encompasses a broad range of potential national security threats, including local, or small-scale wars, regional, or large-scale wars, internal and foreign military threats, the Russian military’s budget, and a host of military-related technical, political, social, and economic issues. Additionally, the doctrine defines the circumstances under which nuclear weapons are to be used by the Armed Forces of the Russian Federation in response to a threat to Russia’s national security.

The current edition of the Russian military doctrine—when compared to the national security strategy and military doctrine published in 1993—significantly lowers the threshold under which the use of nuclear weapons is permitted. While the 1993 doctrine allowed the first use of nuclear weapons only when the “existence of the Russian Federation” is threatened, the versions published since 2000 explicitly state that Russia “reserves the right to use nuclear weapons to respond to all weapons of mass destruction attacks” on Russia and its allies.

Furthermore, the doctrine released in 2000—and all subsequent versions—allows for nuclear weapons use “in response to large-scale aggression utilizing conventional weapons in situations critical to the national security of the Russian Federation.” Succinctly put, Russia’s entire national security strategy is predicated on the concept of nuclear de-escalation.
Historical Context: NATO Intervention in the Balkans

In the year before the release of Russia’s 2000 military doctrine, Russia’s military and political leaders warily observed as NATO executed an efficient and precise conventional military operation in the former Republic of Yugoslavia. In 1999, Russia was facing renewed tensions in Chechnya in the aftermath of the disastrous war that broke out following the Soviet Union’s collapse.

It was clear that the United States (and its allies) possessed far greater conventional military capabilities than Russia. Plus, the underlying ethnic and religious issues in Kosovo which led to NATO taking action were seen by Russia as almost identical to those underlying the first Chechen war. These similarities, combined with Russia’s historical view of Serbia—the successor state to the Republic of Yugoslavia—as its “little brother,” led to Moscow developing deep anxiety that the United States would involve itself in another within Russian borders.

In 2000, Russia released an updated military doctrine in which it outlined the concept of de-escalation through a limited nuclear strike. This idea put forth the notion that if Russia were subjected to a major non-nuclear assault that exceeded its capacity for conventional defense, it would “de-escalate” the conflict by launching a limited—or tactical—nuclear strike. While this policy has never been publicly discussed with relation to any particular conflict, the concept of nuclear de-escalation undoubtedly was on the minds of Western leaders during Russia’s invasion of Georgia in 2008, and in the ongoing conflict in eastern Ukraine.

Conventional and Nuclear Deterrence During the Cold War

The Soviet Union’s collapse and the effective end of the Cold War in the 1990s left Russia and the United States with significantly less reason to fear that one would launch a massive, surprise strategic nuclear attack on the other. The role nuclear weapons played in the international geopolitical framework was fundamentally altered. Nuclear weapons no longer were the centerpiece of security relationship based on the concept of Mutually Assured Destruction (MAD).
Instead, they became status symbols; at the very most, they were considered ultimate insurance policy against unforeseen aggression. Nuclear weapons maintained their role as the penultimate security guarantee; however, they had very much moved to the background of the international security stage. Many, particularly in the West, believed that global nuclear disarmament was an attainable goal.

During the Cold War, deterrence was effective in maintaining peace between the two superpowers because both states ensured that the other would be deterred on all levels in the event of escalating tensions. At the time, the security relationship between the U.S. and the U.S.S.R. was heavily dependent on the concept of parity. Conventional forces were deterred with conventional forces of equal strength, while nuclear arsenals were positioned in support of mutually assured destruction.

As the Soviet Union broke apart, following years of economic stagnation, the United States and its allies were demonstrating their significant conventional military capabilities in their 1990-1991 campaign to expel Iraqi occupying forces from the oil-rich state of Kuwait. Russia's military and political leaders grew increasingly wary about the imbalance—to Russia's disadvantage—in conventional power projection and efficacy.

**Shifting Security Perspectives in the Post-Cold War Era: Russia's Asymmetric Deterrence Strategy**

This anxiety amongst the Russian military's top brass further developed during the U.S.-led NATO 1999 intervention in Kosovo. The United States' conventional military power became a clear and distinct threat to Russia. There were many similarities between the origins of the Kosovo conflict and Russia's own internal war with Chechen separatists during the first Chechen War. What Russia feared most was that the U.S. would intervene in what Russia considered its' internal affairs. If the U.S. were to launch a non-nuclear (i.e. conventional) assault against the newly formed Russian Federation, Russia's conventional forces would be of little benefit.

As nuclear deterrence theory during the Cold War was predicated on the concept of “mutually assured destruction” (MAD), deterrence strategy required that effective and credible forces were maintained at every level—conventional and
nuclear to be effective. The Soviet Union’s collapse decimated that military's conventional force projection capabilities. The subsequent Russian military's ability to deter any conventional U.S. or NATO military action against Russia was rendered ineffective.

The efficacy of the United States' high-precision conventional weapons was demonstrated in both the Balkan and Iraqi campaigns of the 1990s. Unlike nuclear weapons, these precision-guided “smart bombs” were highly usable and effective—in stark contrast to nuclear weapons. Framed in this context, Russia’s military planners became painfully aware of their strategic disadvantage. Thus, the concept of nuclear de-escalation was born.

Before the conclusion of NATO’s Kosovo operation, Russia initiated the development of a new military doctrine that would deter any conventional or nuclear strike against Russia. Responsible for the supervision of this effort was then-secretary of Russia's Security Council, Vladimir Putin. Coincidentally, it was Putin who would sign this doctrine upon its release in 2000, having just become president.

De-escalation revises the scale of a possible nuclear strike. While Cold War deterrence was predicated on the threat of inflicting an overwhelming degree of damage on enemy military and civilian targets, de-escalation rests on the concept of “tailored damage.” The doctrine defines "tailored damage" as inflicting “damage subjectively unacceptable to the opponent exceeds the benefits the expects to gain as a result of the use of military force.” In other words, Russia’s military planners believed that the threat of a limited or tactical nuclear strike against enemy targets would be an effective deterrence against a conventional attack by the United States or NATO.

Today, the concept of “nuclear de-escalation” continues to be in play, presenting a significant challenge to western military strategists. If Russia were to mount a successful invasion of the Baltic states, it is likely that Russia would consider these countries to be sovereign Russian territory, meaning that any conventional NATO military operation designed to restore the independence of the NATO members would likely be met with a limited nuclear strike. That is, of course, unless U.S. or NATO cyber or other non-kinetic capabilities can disrupt Russia's nuclear command-and-control apparatus.
Facebook, Compromised: How Russia Manipulated U.S. Voters

Information Warfare: Russia's "Active Measures."

Conceptually, Information warfare is by no means a new concept. However, the broad reach of social media has created an entirely new and highly effective avenue for Russian ‘active measures’ to penetrate into and influence the minds of the American public. Active measures “employ a three-pronged approach that attempts to shape foreign policy...state-to-people, People-To-People, and state-to-state...The Russian government today uses the state-to-people and people-to-people approaches on social media and the internet.”

According to researchers who conducted a post-mortem of social media activity during the election using internet analytics tools, Russian Information Warfare content on social media attempts to subvert Western democracies in five ways: undermine public confidence in democratic government, exacerbate internal political divisions,

erode trust in government, push the Russian agenda in foreign populations, and create confusion and distrust by blurring fact and fiction. Russian propaganda on social media can be divided into four themes: political messages intended to foster distrust in government (e.g. allegations of voter fraud, corruption), financial propaganda (i.e. create distrust in Western financial institutions), social issues (e.g. ethnic tensions, police brutality), and doomsday-style conspiracy theories.

Information warfare content is generated and disseminated through channels
that fall into three attribution categories: white (overt), grey (less-overt), and black (covert) channels. They propagate a blend of authentic, manipulated, and fake stories and they feed off of and reinforce each other.

White or overt channels include state-sponsored pro-Russian news outlets such as Sputnik and RT, the grey less-overt outlets include data dump sites, such as Wikileaks, and more sinister black channels involve covert operations such as hacking. The agents disseminating the information include bots (automated web robots), and real people, often presenting themselves as innocuous news aggregators. These agents form the key engine for distributing misinformation and disinformation.

Black or covert measures—once highly risky and dangerous to carry out—are now easily and efficiently carried out through social media. Russia is now able to remotely coordinate an army of hackers, honeypots (in this instance, social media profiles used to bait other users into giving compromising or embarrassing information), and hecklers or internet trolls (individuals who purposely create discord or provoke).

The Role of Non-State Cyber Hackers: Advanced Persistent Threat Groups

Cyber hacking groups—or advanced persistent threat (APT) groups—are a critical component of the Kremlin’s information operations. The fact that it is challenging to definitively prove ties to the Russian government is what endears them to the Kremlin. However, while there isn’t necessarily a ‘smoking gun,’ evidence gleaned from previous cyber attacks has allowed the top US intelligence agencies to reach conclusions, with a strong degree of confidence, that the Kremlin was involved.

For example, “the facts that the hackers’ work hours aligned with Moscow’s time zone, operations ceased on Russian holidays, their techniques carried signatures common to other Russian hacks, and their targets were of clear interest to Moscow.”

In the social media realm, hackers provide the fodder for the narratives of disinformation/misinformation generated. “The most notorious Russian-linked
hacker...Guccifer 2.0, targets current and former U.S. government officials, American security experts, and media personalities by seeking access to their private communications and records,” and whatever information may come to light then presents itself in the propaganda created and disseminated.

**Honeypots**

Honeypots are fake social media profiles which are designed to lure in real people to engage with them online: “today’s honeypots may include a component of sexual appeal or attraction, but they just as often appear to be people who share a target’s political views, obscure personal hobbies, or issues related to family history.”

The objective of the honeypot accounts is to earn the trust of unsuspecting users in order to conduct a range of activities including disseminating content from white and gray propaganda channels, attempting to entrap users with compromising propositions such as offers of sexual exchanges, or trying to persuade targets to click on malicious links or deceive people into downloading malware (software intended to damage a computer).

If the target exposed to a malicious link or malware is a person of interest, such as a politician or public figure, this enables APT groups to access personal information and post it on grey channels such as data dump sites. The information revealed in turn helps construct the narrative of misinformation posted on white channels, such as RT or Sputnik, and eventually trickling down to conservative news sites such as Breitbart, before being picked up by the mainstream media.

**Hecklers: Trolls & Troll Farms**

Hecklers, or trolls, give life to Russia’s influence operations. There have been reports of “troll farms,” employing hundreds of people, formed to actively disseminate pro-Kremlin propaganda. It is important to note, “the information contained in the comments and posts by the trolls ranges from misleading to verifiably fraudulent.”

The objective of trolls is not necessarily to defend or validate the pro-Russian propaganda posted, but rather to flood the social media space with such a high
volume of misinformation, as to create a state of confusion and calamity.

Senator Mark Warner, the ranking Democrat on the Senate Intelligence Committee, has said that “there were upwards of a thousand paid internet trolls working out of a facility in Russia, in effect taking over a series of computers which are then called a botnet, that can then generate news down to specific areas.” The implication here: a sophisticated and coordinated social media disinformation campaign was able to micro-target vulnerable voter populations. The reason they were vulnerable is that they received their news from social media, which had been powerfully harnessed to manipulate voters in the critical weeks leading up to Election Day.

**The Ramifications of a Compromised Social Media Space**

Social media, a Western innovation, at a glance seems like an ideal manifestation of a free and open society. Social media platforms enable users to share information, freely express opinions, and connect with other individuals. However, these same platforms were harnessed to wage a full-scale coordinated Information warfare offensive. False articles—“fake news” content—that favored Trump were **four times as likely** to be shared on social media platforms when compared with false stories favoring Secretary Clinton.

“Fabricated pro-Trump stories were shared four times as often as fabricated pro-Clinton stories...researchers also found that roughly half the readers of a fake news story believed it...automated Twitter accounts, known as “bots,” generated four tweets in favor of Trump for everyone in favor of Clinton...a substantial number of these bots were aligned with individuals and organizations supported, and sometimes funded, by the Kremlin.”

Russia utilized generations’ worth of acquired expertise in the art of Information warfare and adapted it to social media in a way that was agile, penetrating and efficient. There is evidence suggesting there were efforts to suppress voters in key precincts in Pennsylvania, Michigan, and Wisconsin.

**These states, which were crucial** in determining the winner of the Presidential election, were flooded with disinformation in the week leading up to the election. While it is difficult to conclusively demonstrate a causal relationship
between the election results and Russian active measures targeted at these populations, it is highly likely, given that all three states voted Democrat in the past 5 Presidential elections.

Donald Trump, a fringe candidate with a radical platform, emerging victorious in these historically moderate voting districts, begs the question of what was the variable that impacted the election? The penetration of Russian Information warfare efforts, so effective due to the successful harnessing of social media, increasingly seems to be the culprit. However, the social media-facilitated assault on the democratic process had another devastating angle: the Trump campaign.
Cambridge Analytica: The Darker Side of Big Data

The "election management" company uses big data and psychometric profiling in operations designed to suppress voter segments.

Before closer scrutiny of the implications of the Trump campaign’s use of Cambridge Analytica’s services, it is imperative to grasp the methodology behind Cambridge Analytica’s services fully. The two fundamental concepts underlying the ‘election management’ company is Big Data and psychometrics: “Big Data means, in essence, that everything we do, both on and offline, leave digital traces...every movement we make...every "like" is stored.” While psychometrics “focuses on measuring psychological traits, such as personality.”

How these two concepts intertwine is crucial to an understanding of what Cambridge Analytica claims to do. Using the OCEAN model, an acronym for personality traits considered the ‘“Big Five’...openness (how open you are to new experiences?), conscientiousness (how much of a perfectionist are you?), extroversion (how sociable are you?), agreeableness (how considerate and cooperative you are?) and neuroticism (are you easily upset?),” relatively accurate assessments can be made about a person. The Big Data facet came into play with the work of Cambridge Ph.D. student Michal Kosinski.

According to reports, Kosinski helped build an app called MyPersonality, which was designed to create “personality profiles” for users filling out psychometric questionnaires. Millions of people participated in the survey and had the option to share their Facebook profile data with the researchers.
Kosinski and his partner were reportedly in possession of “the largest dataset combining psychometric scores with Facebook profiles ever to be collected... Kosinski proved that by an average of 68 Facebook ‘likes’ by a user, it was possible to predict their skin color (with 95 percent accuracy), their sexual orientation (88 percent accuracy), and their affiliation with the Democratic or Republican party (85 percent).”

Not only does the data create a psychological profile, but the methodology can also be used as a ‘people search engine,’ or mechanism for microtargeting: narrowing down results based on desired personality characteristics.

Kosinski’s findings supposedly paved the way for the technology that is currently a significant selling point for Cambridge Analytica, and this was not a coincidence. Aleksandr Kogan, a lecturer at Cambridge University, approached Kosinski in early 2014. Kogan, who was contracted by Cambridge Analytica’s parent company SCL, took an interest in Kasinski’s work and as reported by The Guardian, introduced SCL to Kasinski’s methodology. While Kasinski refused to do business with SCL, it appears that Kogan mimicked his methods:

“Kogan had arranged for more than 100,000 people to complete the Facebook survey and download an app... obtained data from 185,000 survey participants as well as their Facebook friends... and that it yielded 30 million available profiles... No one in this larger group of 30 million knew that “likes” and demographic data from their Facebook profiles were being harvested by political operatives hired to influence American voters.”

SCL—and Cambridge Analytica, by extension—were given an immense amount of usable personal data, obtained without the knowledge or consent of the vast majority of harvested user profiles. According to political communications expert Emma Briant, this ethically dubious behavior is an exploitation of users’ dependence on social media and can be used to manipulate the public. Currently, Cambridge Analytica claims to have “a database of 230 million American adults, with up to 5,000 pieces of demographic, consumer and lifestyle information about each.” The company markets its services based on claims of being able to influence voter behavior with “microtargeting.”
The Trump campaign paid Cambridge Analytica millions of dollars during the election process, and interestingly, Stephen K. Bannon, Trump’s Chief Strategist and former head of Breitbart News (which was mentioned earlier as an active participant in spreading Russian-generated misinformation/disinformation), used to sit on Cambridge Analytica’s board.

**The Implications of “Microtargeting”**

According to a recent scientific analysis by Kosinski, individually tailored Facebook advertising based on personality targeting can attract up to 63 percent more clicks and up to 1,400 more conversions. These statistics reveal the implications of any campaigning politician possessing social media microtargeting capabilities. Social media enabled the delivery of strategic information, without knowledge or consent, to a company whose objective is to exploit users’ data to influence voter behavior.

Crucially as well, social media provided the access Cambridge Analytica needed for their microtargeting campaigns to reach the intended audience. In the words of Professor and data scientist Jonathan Albright, “This is a propaganda machine. It’s targeting people individually to recruit them to an idea. It’s a level of social engineering that I’ve never seen before. They’re capturing people and then keeping them on an emotional leash.”

The way in which Cambridge Analytica operates is insidious and often invisible, “leveraging automated emotional manipulation alongside swarms of bots, Facebook dark posts, A/B testing, and fake news networks.”

Senator Mark Warner’s statement once again comes to mind: reports presented to the Senate Intelligence Committee alleged that voter suppression campaigns on social media were targeted with precision down to the precinct level in crucial battleground states. Aiding in voter suppression efforts is nothing new for SCL (Cambridge Analytica’s parent company), which reportedly provided its services to support a voter suppression campaign in Nigeria.

The ramifications of these revelations are highly significant. Social media and Big Data analytics are changing the way in which political candidates conduct their campaigns. The personal information and preferences shared on social
media leave voters vulnerable to influence, and Big Data allows politicians to know exactly which buttons to push.

**The West's Critical Vulnerabilities to Information Warfare Operations**

While it is beyond the scope of this work to definitively prove intentional collusion between the Russian government and the Trump campaign (although evidence continues to emerge at the time of publication), there is ample information to substantiate that there were unsavory influence campaigns conducted on both sides.

To better understand the Russian angle, this analysis outlined the concept of Russian Information Warfare and elucidated the critical difference in its conceptualization between Russia and the West.

It emerges that this contrast has led to a security gap in Western cyber strategy: there has been too much of a focus on the technical aspects of cyber threats. While the US was trying to protect voting machines from getting hacked, the actual voters were the ones left most vulnerable. It becomes evident that social media not only made activities for generating disinformation/misinformation easier, but it facilitated its dissemination with penetrating precision and efficacy.

The second part of this work examined how the Trump campaign harnessed social media in two ways. Firstly, Trump exploited his status and power to legitimize Russian active measures; social media was vital in providing an avenue of communication with a direct audience of over 46 million.

Secondly, the Trump campaign used Big Data 'election management' company Cambridge Analytica, which uses a database of stolen personal details to micro-target voters, and has a history of running voter suppression campaigns. If the insinuation in Senator Warner’s quote (from the beginning of this paper) is true, according to the panel of experts he asked at the hearing, it is absolutely possible that Russian-hacked voter database rolls could have been used in coordination with.

Social media personal data gives context to the voter registration database
information, and microtargeting tools such as Facebook dark posts allow voter suppression campaigns to be executed with razor precision down to the voting precinct. Cambridge Analytica is only one of a number of similar companies that are emerging. Social media and Big Data analytics are changing the way political campaigns are run, and the sinister side of it is: they know how to pull the right emotional strings to elicit the exact desired response. This is a perversion of the democratic process, especially if fake news, generated by a foreign adversary with the explicit purpose of subverting Western institutions, is used as a tool to influence public opinion.

It should be noted that these implications don’t apply to the US alone. Cambridge Analytica has provided its services to the Leave.eu (Brexit) campaign, two US Presidential election candidates, countries in Africa and the Caribbean, and their client list is only growing in light of their runaway success. In parallel to these revelations,

Russia has also poured resources into Brexit, the US election, as well as French, Dutch, German, and Austrian far-right political parties.

Russia is aggressively pursuing a political agenda, and their expertise in the cyber domain is just a facet of a sophisticated grand political and military strategy—a demonstrable threat to liberal democracy. The West needs to adapt to the changing cyber landscape and begin to perceive threats differently. Cyber is much more than just the technical or the hardware. The exploitation of social media in the 2016 US Presidential election proved to be the perfect example of how information can be weaponized to swing an outcome and achieve a desired strategic objective.
Russian FSB Official Linked to DNC Hack Charged with Treason for "Aiding CIA"

Senior FSB agents accused of treason after Kremlin insiders dismissed the Steele dossier as "gossip."

Seven days after Trump’s inauguration, a stream of reporting emerged from independent Russian media outlets. On January 27, 2017, Novaya Gazeta reported that Sergei Mikhailov, the Deputy Chief of the cyber unit in the successor agency to the KGB—officially the Information Security Department of the FSB—was in attendance at a meeting of high-level FSB staff during the first week of December. In that meeting, security personnel suddenly entered and grabbed Mikhailov, placed a light-proof bag over his head, and dragged him from the room.

Mikhailov hasn't been seen since, and Interfax, the independent Russian newswire, has corroborated the story, which quotes an anonymous FSB official saying that Mikhailov and his deputy Dmitry Dokuchaev, were accused of “breaking their oath and working with the CIA.”

However, it was reported sometime later that two sources indicated that he may have been an asset for a foreign intelligence agency inside the FSB. On February 1, charges of high treason on behalf of the United States were brought to them. Again—in this case citing investigators—Dokuchaev and Mikhailov were thought to have cooperated with the CIA. The men are alleged to have “transferred confidential data to the American...
company Verisign and to other commercial organizations which in turn transferred these data to intelligence agencies of the USA”. Representatives from VeriSign did confirm that data was received by the company, although stated that it was not confidential in nature.

According to *Novaya Gazeta*, Mikhailov specifically passed along information about Vladimir Fomenko, owner of Kings Servers, to U.S. intelligence officials. This information was regarding Fomenko's involvement in the cyberattacks on the electoral systems of Arizona and Illinois. At the same time, Interfax news agency reported that an additional 8 people had been identified by the FSB as accomplices.

**The Mystery of the Seven Dead Russian Diplomats**

Since election day in November 2016, seven Russian diplomats—including Russian ambassador to the United Nations Vitaly Churkin, and ex-KGB head Oleg Erovinkin—have been killed or found dead in increasingly questionable circumstances. Churkin’s death is under investigation by the New York City medical examiner, while Erovinkin—who is believed to have assisted Christopher Steele with compiling the now-infamous kompromat dossier—was found dead in the back of his Lexus.

The goal of Russian interference in the American election was to foment disillusionment with democratic institutions—to delegitimize Western political systems. Within the Kremlin, officials originally believed that Hillary Clinton would win the United States' 2016 presidential election. Russia’s interference strategy was intended to shape a political climate so rife with mistrust and division that a Clinton administration would be forced to concentrate on ensuring domestic policy and stability, at the expense of American foreign policy interests.

The lack of planning in the event of a Trump victory created, rather than solved, a new problem for the Kremlin. The U.S. federal government’s executive branch has become increasingly unpredictable, a stark departure from the decades of more-or-less predictable U.S. foreign policy to which the Kremlin has become accustomed. As President, Trump is not the authoritarian that Putin is able to be.
Military power is largely in the hands of Secretary of Defense Mattis, having been given a near-unprecedented degree of autonomy in directing military operations by Trump.

Furthermore, the Kremlin seems ill-prepared for an operation of this magnitude, ostensibly having failed to understand the strategic (long-term) implications for sponsored institutional disruption in a state (the U.S.) with bureaucratic and democratic institutions designed to impede would-be authoritarians. In Russia, such leaks do occur, albeit with greater consequences.

**Strategic Analysis: Growing internal friction and high profile moles within Russia's security services diminishes their ability to maintain order—and power.**

As Russia's economy declined after having enjoyed a hot streak during the early 2000s, thanks to skyrocketing commodity prices, Putin's foreign policy devolved into a projection of Russian hard power, with the intent of rebuilding national pride in a resurging global power.

As the 2018 presidential election approaches, protests and dissent are growing throughout Russia. Typically, Moscow's and Saint Petersburg's middle class and opposition elites are the typical protesters; they have greater access to the West and its social networking and media, and are more exposed to democratic ideas.

The majority of Russians, however, receive news and information through state-managed channels, and many are dependant on state institutions for employment or pensions. Living in the "Regions" (industrial, non-cosmopolitan cities, towns, and villages, excluding the two main cities), most Russians have experienced a sharp decline in their standard of living.

Russia's Gross Domestic Product (GDP), per capita, has dropped over 41% from its 2013 height of $15,543. For a country having suffered through a corrupt transition from the Soviet control economy in the early 1990s, followed by a complete economic collapse in 1997, an ongoing major decline, overseen by a kleptocratic elite would likely result in a large degree of public unrest and resistance.
Historically, the Kremlin manages internal unrest by harnessing Russian nationalism and engaging in conflict abroad, under the guise of protecting Russian security interests, or restoring Russia as a global "great power." The key for the Kremlin, and ultimately, Putin, is to make sure that these campaigns generate tangible rewards for the Russian electorate.
Trump’s Attempt to Co-Opt the National Security Agency has Backfired

NSA Director Admiral Mike Rogers: SIGINT exists that answers the Trump-Russia collusion question.

Admiral Mike Rogers, Director of the United States National Security Agency recently held a “town hall” meeting with agency employees. The teleconference was broadcast to Agency facilities worldwide—apparently, a rarity.

The Observer reports that Admiral Rogers detailed to employees how Donald Trump attempted to coerce him into denouncing the FBI and Director Comey, according to multiple sources within the agency, all speaking on the condition of anonymity.

Sources report that Rogers explicitly stated that signals intelligence (SIGINT) that could support claims of collusion between Trump and company, and the Kremlin. Two additional NSA employees—employed in different capacities, and contacted independently of one another—have verified this to Global Security Review, validating the version of events as described below.

"I know you won’t like it, but I have to tell what I have seen."
- NSA Director Admiral Mike Rogers to President Trump

Rogers explained how President Trump sought out both Admiral Rogers’ and Director of National Intelligence Dan Coates to publicly discredit former FBI
Director James Comey, and the FBI, itself. Rogers adamantly refused to comply with the President’s request. Reportedly, Rogers then said to the President (again, independently validated to us by two separate agency employees): “I know you won’t like it, but I have to tell what I have seen.”

The same sources confirmed the report that Rogers (speaking to agency employees) explained that SIGINT does exist that is damaging to the Trump team. They verified that Rogers said “there is no question” the agency possesses SIGINT that evidences coordination between the Trump campaign and the Kremlin with regards to the 2016 presidential election.

**NSA Ramps Up Its Support in the Investigations**

The NSA has not only passed this intelligence along to the FBI counterintelligence and criminal investigation teams but has taken near-unprecedented measures to ramp-up investigative efforts.

Multiple sources have shared (initially with *the Observer*) that a preservation order had been issued to the NSA’s Directorate of Operations, the largest unit within the agency; responsible for managing and coordinating the agency’s SIGINT collection and operations assets around the globe.

A preservation order is a rarity within the NSA—agency insiders say the severity of the investigations is underlined by that fact. The preservation order—sent from the NSA’s General Counsel’s office—directs directorate personnel (at all levels) with identifying and preserving any SIGINT records that relate—even indirectly—to the allegations of improper ties between the Trump campaign or administration and Kremlin officials.

The order, according to multiple sources within the Directorate of Operations, specifically charged NSA analysts, managers, and other officials with seeking out (and preserving for investigators) any references to anyone who may have had the slightest involvement—especially to U.S. officials—with the Trump-Russia scandal.

Sources report that records would include intercepted emails, telephone call
records, phone call transcripts, instant messages, social media posts or private messages, faxes, and anything else that might have been intercepted by the NSA. Sources have requested that individuals named in the General Counsel’s preservation order not be publicized as this

Sources have requested that individuals named in the General Counsel’s preservation order not be publicized as it pertains to ongoing criminal and counterintelligence investigations.

**What does this mean for U.S. National Security?**

The investigation seems to be ramping up. A prolonged investigation isn’t in U.S. national security interests, particularly considering Admiral Rogers recent comments. Top secret information could have been transferred to the Kremlin, or there may be further schemes afoot. Speculation aside, the U.S. information security is at risk as long as this investigation is underway.
Donald Trump Jr's Secret Communications with Wikileaks

Newly discovered communications between Donald Trump Jr. and Wikileaks during the 2016 campaign reveal a coordinated effort to distribute information damaging to the Clinton Campaign.

- Wikileaks is considered to be a non-state intelligence agency with hostile intentions to the United States and ties to Russian military and foreign intelligence agencies.
- Wikileaks asked Donald Trump Jr. for his cooperation in coordinating the distribution of political messages, in contesting the results of the election, and in sending “the right signals” to U.S. allies like Australia and the U.K.
- These revelations indicate some form of coordination between a Kremlin actor and the Trump campaign.
- At the strategic level, these communications centered on building a sustainable narrative that would be mutually beneficial for the Trump Campaign, Wikileaks, and their respective backers.
- Steve Bannon, Kellyanne Conway, Brad Parscale, Hope Hicks, and Jared Kushner were informed of these communications during the campaign.
- Wikileaks’s suspected involvement with Russian military and security intelligence services was public knowledge at the time.

The Atlantic Magazine published a set of private communications between
Donald Trump Jr. and Wikileaks. These messages were sent prior the election and discussed how best to disseminate the trove of DNC emails obtained by Wikileaks through a Russian Intelligence hacking operation.

The messages reveal a lengthy and often one-sided correspondence between Wikileaks and Donald Trump Jr. that continued until sometime July 2017, at least. The U.S. intelligence community believes that Wikileaks was either playing a complicit or ignorant role in disseminating information obtained by Russian intelligence services. The CIA Director, Mike Pompeo, labeled Wikileaks as a “hostile non-state intelligence agency” at his first public remarks as CIA Director at the Center for International and Strategic Studies.

In the messages, Wikileaks asked Donald Trump Jr. for his cooperation in coordinating the distribution of political messages, in contesting the results of the election, and in sending “the right signals” to U.S. allies like Australia and the U.K., “to start following the law and stop bending it to ingratiate themselves with the Clinton’s.”

These revelations indicate some form of coordination between a Kremlin-linked actor and the Trump campaign, mainly as the email conversations between Trump Jr. and Wikileaks were taking place during campaign events and refer to references to Wikileaks. Furthermore, it seems as if the Wikileaks team perceived themselves as working in the capacity a partner of—or even a department within—the Trump Campaign. The view within Wikileaks mostly seemed to be that the two organizations were working in tandem.

The messages allege media strategy coordination by Trump Jr. and Wikileaks.

Julia Ioffe, the author of the Atlantic's piece centers on a specific exchange between Trump Jr. and Wikileaks. On October 3, 2016, WikiLeaks wrote: "Hiya, it’d be great if you guys could comment on/push this story," WikiLeaks suggested, attaching a quote from then-Democratic nominee Hillary Clinton about wanting to “just drone” WikiLeaks founder, Julian Assange.

"Already did that earlier today," Trump Jr. responded an hour-and-a-half later. "It’s amazing what she can get away with." Trump Jr. wrote again two minutes later, asking, "What's behind this Wednesday leak I keep reading
about?"

The day before, Roger Stone, an informal advisor to Donald Trump during the campaign, tweeted: "Wednesday @HillaryClinton is done. #WikiLeaks." WikiLeaks didn't respond to Trump Jr.'s question, but on October 12, 2016, the account again messaged Trump Jr: “Hey Donald, great to see you and your dad talking about our publications,” WikiLeaks wrote.

"Strongly suggest your dad tweets this link if he mentions us,” WikiLeaks went on, pointing Trump Jr. to the link *wlsearch.ttk*, which it said would help Trump's followers dig through the trove of stolen documents and find relevant stories.

“There’s many great stories the press are missing and we’re sure some of your follows will find it,” WikiLeaks went on. “Btw we just released Podesta Emails Part 4.”

**Wikileaks Attempted to Communicate with Trump Jr. As Recently as July 2017**

The communications didn't end with the election. In July 2017, in the wake of Donald Trump Jr.'s congressional testimony, Wikileaks reached out to Trump Jr. again. “Hi Don. Sorry to hear about your problems, We have an idea that may help a little. We are VERY interested in confidentially obtaining and publishing a copy of the email(s) cited in the New York Times today.” The message was referencing a Times' report on emails Trump Jr had exchanged with Rob Goldstone, a publicist who had helped set up the now-infamous June 2016 Trump Tower meeting with Russian lawyer Natalia Veselnitskaya.

"We think this is strongly in your interest,” WikiLeaks went on. It then reprised many of the same arguments it made in trying to convince Trump Jr. to turn over his father's tax returns, including the argument that Trump's enemies in the press were using the emails to spin an unfavorable narrative of the meeting. "Us publishing not only deprives them of this ability but is beautifully confounding."
In short, Wikileaks offered to publish Donald Trump Jr’s (already released) emails to WikiLeaks in an attempt to show that Wikileaks is objective concerning the targets of their “leaks.” Secondly, this would benefit Trump Jr. as he could use Wikileaks’s reputation as a hostile non-state intelligence service to his advantage, by claiming that the emails were doctored or otherwise misrepresented. Unfortunately for Wikileaks, Trump Jr. proceeded by posting the emails to his own twitter account.

**Analysis: while mostly one-sided, the communications imply coordination between the Trump Campaign and Wikileaks**

The conversations centered on how surrogates or the candidate was referring to specific keywords or hashtags in social media postings. At a technical level, this would indicate coordinated action by the trump campaign with Wikileaks. Beyond these emails, the extent of coordination that has taken place is unclear at this point. At the strategic level, these communications centered on building a sustainable narrative that would be mutually beneficial for the Trump Campaign, Wikileaks, and their respective backers.

While the communications between Trump Jr. and Wikileaks are not necessarily a legal offense (Trump Jr. was a private citizen at the time), if he failed to provide information or documents to the special counsel or congressional investigators, he may be liable for obstruction of justice.

**Who Knew What, and When?**

What’s important to draw from these exchanges is that while Donald Trump Jr. in large part ignored emails from Wikileaks, he did act on some of their requests. According to Ioffe, the same day that Donald Trump Jr. received the first email that was sent by Wikileaks, he informed senior Trump Campaign officials. Specifically, Steve Bannon, Kellyanne Conway, Brad Parscale, Hope Hicks, and Jared Kushner all became aware of Trump Jr.’s contacts with Wikileaks. Donald Trump Jr. did not rebuff Wikileaks at any time during his correspondence with the organization. Wikileaks’s suspected involvement with Russian military and security intelligence services was public knowledge at the time.
The Subtext of Secretary Mattis' Mysterious Memo

After a cryptic department-wide memo some are asking if Secretary James Mattis is trying to send a message.

Early in August and without pretext, Secretary of Defense James Mattis circulated a memorandum to Defense Department staff stressing the importance of ethics, saying he expects all staff, uniformed and civilian, “to play the ethical midfield.”

The Department did not provide any further specificity regarding Secretary Mattis’ motives in sending the memorandum. What prompted Mattis’ memo?

Mattis’ framing of the idea of training as mindfully engaging in ethical conduct—at all times—could be interpreted as a subtle nod towards potentially trying events to come. Events, where the Department of Defense, must maintain its integrity and ethical responsibility at all costs. (see next page for memo)
Also worthy of recognition is Mattis’ point about upholding the trust that others place in the organization. The trust Mattis speaks of is far more valuable and significant than the trust an employee has in an employer.

He speaks of the faith the American people have in their armed forces in their ability to protect them and the national security of the United States.
The legitimacy of the U.S. is partially guaranteed by its supposedly civilian-controlled military, and Mattis (while a retired 4-star general) knows that trust and legitimacy must be maintained at all costs.

**Why was the memo distributed?**

One assessment is that Mattis could be telegraphing a message that staff should still respect and work with transgender employees. Other military leaders have already begun dismissing the president’s directive.

Another read of the memo is that Mattis is warning DoD employees against obeying any illegal orders that Trump might soon issue, on Twitter or otherwise. One can’t dismiss that idea either, especially since Congress just departed for August recess. If Trump wanted to try something crazy (firing attorney general Jeff Sessions and special counsel Robert Mueller, for example), now would be a natural time for him to do so.

Mueller has convened a grand jury to keep pressing the investigation into possible collusion between the Trump campaign and the Russian government. Subpoenas are flying. Document requests have been sent. One target of the investigation seems to be erstwhile national security adviser Michael Flynn, who served in the Army for 33 years until he was forced out in 2014. Then he began his second career shilling for Russia and Turkey.

Department employees or serving members of the armed forces may have documents in their files that Mueller wants to read. Mattis may be reminding them that, even in these bizarre and difficult times, they are duty-bound to do the right thing.
Trump Campaign Officials Indicted in Special Counsel Investigation

Trump Campaign Chair and associate were charged on 12 counts, including conspiracy against the United States and money laundering.

Special Counsel Robert Mueller has indicted Former Trump Campaign Chairman Paul Manafort on 12 counts, including conspiracy against the United States, conspiracy to launder money, and for making false and misleading Foreign Agent Registration Act (FARA) Statements. Richard Gates III, an associate of Manafort, was also indicted.

The indictment alleges that Manafort and Gates funneled over $75 million through offshore accounts and that Manafort himself laundered more than $18 million to fund property acquisitions, home renovations, and private school tuition.

Manafort and Gates are alleged to have received tens of millions of dollars in income as political consultants in Ukraine. The indictment states that to hide that income, they laundered it through "scores of United States and foreign corporations, partnerships, and bank accounts." Manafort and Gates consulted pro-Russia Ukrainian politicians on lobbying, public relations, and political strategy. Gates is referred to as "Manafort's right-hand man" in the 32-page indictment.
Political Consulting in Ukraine

A primary focus of their work in Ukraine was the advancement of the pro-Russia Party of Regions, and their presidential candidate Viktor Yanukovych, who would be elected in 2010. Yanukovych would later flee to Russia in 2014 amidst widespread uprisings in Ukraine.

In the indictment, Mueller highlights an entity called the European Centre for Modern Ukraine as "a mouthpiece for Yanukovych and the Party of Regions." It is alleged that the Centre was part of a "cover story" that was developed by Manafort and Gates to distance themselves from their work in Ukraine.

U.S. law mandates that when American citizens are engaged in work for a foreign country, they must register as foreign agents of that state, as stipulated under the Foreign Agents Registration Act (FARA). Neither Manafort nor Gates registered as foreign agents during their time working as consultants for then-President Yanukovych.

Manafort and Gates initially stated to FBI investigators that their role was to introduce various companies to the Centre and that their efforts did not include lobbying work on behalf of the Party of Regions within the United States. However, the indictment alleges that Manafort and Gates not only selected the companies that would conduct the work on behalf of Yanukovych, but they also engaged in weekly calls and email communications to direct the steps that would be taken by the lobbyists. The indictment alleges that Manafort and Gates paid lobbyists more than $2 million from offshore accounts to conduct work on behalf of Yanukovych and the governing pro-Russia Party of Regions within the United States.

Asset Forfeiture

A critical aspect of the indictment is that Special Counsel Mueller is seeking the forfeiture of assets obtained using laundered money on which no taxes were paid. The assets listed in the charges include a life insurance policy, and multiple properties, including Manafort's residences in Virginia and the Hamptons, New York.
Crisis in Venezuela: Economic Collapse, Violent Unrest, and Human Survival

Venezuela is in the throes of a political and economic crisis. By no means a newfound concept for Venezuelans, this time is different.

As the conflicts in Ukraine and the Middle East, and the threat of escalations on the Korean Peninsula continue to draw the majority of international media attention, Venezuela’s deepening political and economic crisis rapidly grows regarding significance for security in the Americas.

To understand the complexities the perfect storm of food and economic insecurity, political repression, and violence stemming from the absence of any form of law and order, we spoke to Jennifer McCoy, Ph.D., distinguished University Professor of Political Science at Georgia State University. Dr. McCoy served as Founding Director of the Global Studies Institute at GSU (2015-16), and Director of the Carter Center’s Americas program (1998-2015) where she led projects strengthening democratic institutions, provided mediation and encouraged dialogue and hemispheric cooperation. Her latest book is *International Mediation in Venezuela* (co-authored with Francisco Diez, 2011).

Dr. McCoy directed the Carter Center’s projects on Mediation and Monitoring in Venezuela (2002-2004), the Ecuador-Colombia Dialogue Group (2008-2010), and the U.S.-Andean Dialogue Group (2010-2011), and led over a dozen election
monitoring and observation missions.

The Current Situation: Repression, Resource Insecurity, and the Risk of Escalation

According to Dr. McCoy, three main scenarios could potentially play out. One of these is the current situation; people willing to publicly protest led by a unified opposition with specific demands are being met by the government with repression. If no concessions are made by the government, the unrest could potentially peter out if no change occurs.

*The Maduro government has been hanging on... waiting for oil prices to rise... trying desperately to make its bond payments...*

This has happened twice before in the past three years. Venezuelan’s went out into the streets, drawing international attention, and resulting in dialogues that were sponsored by the international community. Each time, an exchange was sponsored and then protests died down, but nothing was changed as a consequence of the inter-party dialogues. The government and its economic policies continued, the social situation deteriorated, and the stage was effectively set for another crisis like the one we see now.

But what makes this round of protests really different and more sustained is the lack of elections as an alternative means to resolve differences. The cancellation of all election options, as well as the Supreme Court's undermining the authority of the legislature (the only institution controlled by the opposition), means the people are losing hope of peaceful means of changing the situation.

Russia and China have provided the Venezuelan government with financial support as it tries to hang on. The government is counting on the situation to improve—i.e. for oil prices to rise—before the presidential elections scheduled for late-2018. They've already delayed or all-out suspended local, regional, and governor elections and successfully halted an effort by the opposition to have a recall referendum that would cut short the president’s term.

*Source: Jennifer McCoy, Ph.D., Distinguished University Professor of Political Science at Georgia State University. Dr. McCoy served as Founding Director of the*
Global Studies Institute at GSU (2015-16), and as Director of the Carter Center’s Americas program (1998-2015) where she led projects strengthening democratic institutions, provided mediation and encouraged dialogue and hemispheric cooperation. Her latest book is International Mediation in Venezuela (co-authored with Francisco Diez, 2011).
How Likely is a Civil War in Venezuela?

The worst-case scenario for Venezuela: Prolonged economic crisis and food shortages, coupled with rapidly escalating violence and unchecked arms proliferation could lead to a civil war

If there isn’t any meaningful resolution of the crisis or an abatement of public anger, Dr. Jennifer McCoy, Distinguished University Professor of Political Science at Georgia State University, says a significant escalation in tensions and armed conflict is possible, from what is currently mainly peaceful protests with low levels of violence.

Harsh repression has been widely propagated by the government or by government-armed militias and gangs. However, the risk of escalation increases due to the large number of young Venezuelans that are coming out and setting up barricades in the streets, mainly in the evenings after protests have ended, and engage in fights with police, the National Guard, and the government-armed gangs.

Dr. McCoy notes that the youths coming out in opposition aren’t using firearms. Rather, they’re using Molotov cocktails, sticks, and are setting fires in the streets. The danger here is if this low-level of violence escalates and spirals out of control with increasing levels of chaos and violence between civilian protesters, the political opposition, government-armed militias and street gangs, and government police and military forces.
Is Venezuela the Next Syria?

In some ways, it is possible Venezuela’s situation could escalate to the level currently observed in the Syrian civil war. That would be the absolute worst-case scenario, according to Dr. McCoy, with some key differences. Both crises arose from food and resource shortages, but ethnic and religious factions—like those engaged in the Syrian civil war—don’t exist in Venezuela.

In Syria, the military has supported Assad partly because of the ethnic and religious alignments in the region and—to some degree—the belief that the armed forces best chances of survival lay with Assad. In Venezuela, the socialist Chavez movement arose from the military. It was when it incorporated some civilian leftist intellectuals that it became a hybrid civic-military coalition movement.

The Venezuelan military, however, has a long professional history, and members of the armed forces have been very reluctant to fire on their citizens, and have been pushing for the military to maintain the legitimacy and professionalism of the institution of the armed forces. Still unclear, however, is the degree to which the military has been politicized in Venezuela.

Since Chavez and his supporters came to power 15 years ago, they’ve made political promotions within the military, but it is unclear how far lower-ranking troops, who are also suffering from low salaries and food and medicine shortages, will support their superiors if they are called on to repress their fellow citizens.

Regional Geopolitics and the Venezuelan Crisis

Geopolitically speaking, the situation in Venezuela is much different than the conflict in Syria. Venezuela’s neighbors are democratic. The Maduro government is also very conscious of legitimacy; it doesn’t want to be seen as an authoritarian regime—and a military takeover would carry the stigma associated with an authoritarian ruler. In this day and age, military coups aren’t as accepted in the Western hemisphere.

While the worst case scenario is Venezuela devolving into civil war, Dr. McCoy
believes that point is still some ways off. Venezuela’s democratic neighbors—
Columbia, or Brazil, for instance—would likely exert tremendous pressure on the
government and security services in Venezuela to negotiate an end to hostilities
before it escalates into a full-blown civil war.

If the worst is to occur, with continued failures of the state to govern effectively,
if the country enters a state of general lawlessness, then there will be
repercussions for the entire hemisphere, as well as Europe, Dr. McCoy says. While
Venezuela doesn’t produce drugs, it’s a major transport hub for drugs going to
Europe and even to Africa before making their way to Europe.

Drug trafficking increases under lawlessness, as we saw in Honduras after 2009.
There was a coup, and for a while, the country was run by a very weak
government, and lawlessness increased dramatically. Now, Honduras has one of
the highest homicide rates in the world. Countries like the United States are
seeing a significant increase in the number of people arriving from countries like
Honduras that are plagued with violence. An actual collapse of the state in
Venezuela would likely mean large numbers of economic migrants and refugees
fleeing the violence.

Particularly, the Venezuelan border with Colombia would be most fragile. For a
while, Venezuela closed the border with Colombia as thousands of people would
try to cross the Amazon into Colombia just to try and get food or medicine.

If the security situation in Venezuela worsens, the Colombian border would be
the main point where people would cross. Internally, Colombia is just starting to
get its peace agreement in place, so further destabilization in Venezuela could
have significant ramifications for Colombia.

Source: Jennifer McCoy, Ph.D., Distinguished University Professor of Political
Science at Georgia State University. Dr. McCoy served as Founding Director of the
Global Studies Institute at GSU (2015-16), and as Director of the Carter Center’s
Americas program (1998-2015) where she led projects strengthening
democratic institutions, provided mediation and encouraged dialogue and
Forget about North Korea, Venezuela is the next major national security crisis

The country has become a full-blown narco-state, making a negotiated political settlement nearly impossible.

Venezuela’s problems will only get worse as President Nicolas Maduro strips Venezuela’s democratic institutions of their authority while consolidating his power. While government and business elites who have access to petrodollars enjoy overwhelmingly favorable exchange rates, the majority of Venezuelans are going hungry.

- **Government mismanagement of the oil industry is at the root of Venezuela’s humanitarian crisis, as productivity has rapidly collapsed.**
- **Hyperinflation has made Venezuelan currency nearly worthless as the prices of essential goods have skyrocketed.**
- **If the already-dire situation worsens considerably, there will be a massive overland exodus of refugees from Venezuela to Colombia, Brazil, Guyana, and the United States.**
- **The number of Venezuelans seeking political asylum in the United States has increased by over 160% from 2016.**

Already, thousands have fled, and the number of Venezuelans seeking political asylum in the United States has increased by over 160% from 2016. As food insecurity worsens for the public and the government steps ups its repression of dissent, there will be a spillover effect regarding migration to the United States from South and Central America.
If the United States is unprepared for such a crisis, the results could have catastrophic implications for American national security. The Venezuelan Vice President, Tareck El Aissami, has been accused of having ties with Iranian and Hezbollah connected individuals and entities. El Aissami has been linked to 173 Venezuelan passports and identity cards that were issued to individuals from the Middle East and Central Asia, including alleged members of Hezbollah.

Holders of Venezuelan passports are afforded visa-free entry to over 130 countries, including 26 European Union member states. While a visa is required to enter the United States, there are likely more lenient standards for accepting applications from holders of Venezuelan passports than for holders of Iranian, Syrian, or Lebanese passports.

The situation in Venezuela is terrible for everyone

For Venezuela, the worst case scenario is a complete breakdown of the central government’s control over the state. If the Venezuelan government is unable to contain the flow of refugees and an overwhelming number cross into neighboring Brazil and Colombia, those governments may be forced to act in the interest of their national security interests.

Given the geographic proximity of the United States to Venezuela, democratic governance there along with adherence to the rule-of-law is paramount for American security in the long-term. Otherwise, the U.S. will undoubtedly face a massive influx of immigrants. Such a flow would not be stopped by a wall, like the one proposed by President Trump along the U.S.-Mexico border. Venezuelans seeking refuge from the humanitarian crisis will utilize air or maritime transport routes to reach the U.S.

Already, over 250,000 Venezuelans have migrated into Colombia in search of greater security and access to food and medical care. Colombia is in the process of finalizing a significant peace agreement with the FARC Rebel group, and a continued mass-migration of Venezuelan refugees could threaten Colombia’s internal stability. Absent a political settlement, which seems increasingly impossible due to the criminal nature of the Venezuelan regime, military intervention may be the only solution. The Colombian government—possibly in cooperation with Brazil and other regional partners—may decide to pre-empt a
mass-exodus of Venezuelans into Colombia by launching a military operation with the intent of deposing the government of Nicolas Maduro.

This would be no easy task. Venezuela, in addition to its military resources, has close security ties with Cuba. An attempt at intervention in Venezuela by a coalition of American democracies could rapidly descend into a much more significant conflict, mainly if hardliners in Havana perceive the operation as an American-led proxy war directed against Cuba and Cuba's overseas interests.
China’s Economy on Unstable Ground: Debt Skyrockets as Unemployment Spreads

For the first time in years, the S&P has lowered China’s credit rating to an AA- with a negative outlook.

- Over two million Chinese workers have been laid off in recent months due to “over capacity.”
- Companies have been shut down as employers either sold their businesses or simply disappeared.
- These layoffs have increased the numbers of unemployed youth in urban areas, increasing the risk of social unrest.
- Chinese President Xi Jinping has suggested sending China’s increasingly debt-prone youth to work in the country, in a “Second Cultural Revolution.” Few have taken the offer despite employment opportunities in farming, food processing, and rural tourism.
- Industrial manufacturing—comprising approximately 45 percent of China’s GDP—is suffering from debt-laden overproduction. Chinese corporations owe an aggregate amount equivalent to 170% of China's GDP.

China’s economy appears to be on shaky ground, as layoffs increase and consumer debt levels and capital flight skyrocket.

The state-supported National Institute for Finance and Development (NIFD) stated earlier this year that local and provincial governments, small businesses, and households owe an amount totaling 154 trillion yuan (almost $23 trillion)—228 percent of China’s GDP. The NFID estimates that household debt alone is
projected to reach 66 trillion yuan ($8.45 trillion) within the next three years.

Corruption, Speculation, and Money Laundering

Economists and media pundits within China have recently escalated rhetoric critical of financiers and industrial elites. Wang Xiangwei, a Beijing-based media pundit, harshly criticized speculators and financial tycoons for their prolific exploitation of regulatory loopholes and government connections.

In the South China Morning Post, Wang wrote that these speculators secured cheap loans for themselves while issuing high-risk financial products to finance projects and investments both within and outside of China.

Furthermore, China’s wealthy have begun moving massive amounts of capital abroad, under the guise of the government’s call for investing overseas—termed “going out.” A particular tactic being used is inflating the value of one’s domestic assets and guaranteeing these funds to overseas branches of Chinese banks, which in turn provide them with overvalued loans which finance asset acquisitions abroad.

Lay-Offs and Labor Disputes

China’s massive labor force has enabled it to become the globe’s manufacturing hub, creating massive domestic economic growth. Unemployment insurance covers only about 10% of China's 270 million migrant workers according to the Chinese Government’s statistics agency.

Lin Yanling, of the Beijing-based China Institute of Industrial Relations, says that “the size of China’s labor force has peaked, but it’s wrong to think that there will be no employment problems.” Lin said 80% of China’s workers are “in a weak position” regarding their job and wage security, adding “if the economic situation is not good, their position will become even weaker.”
China's economy is heavily export-driven. Competition from countries offering lower-wage workforces will have an impact on workers in the manufacturing sector.

Any mass-disruption for manufacturing workers, migrant workers, or other low-wage worker is bound to have consequences for internal stability that could prompt a forceful intervention by the government. This and ongoing wage stagnation are the two issues of greatest concern. Thus, the government’s efforts to resettle urban unemployed in the country through offers of paying jobs could be a preemptive attempt to avoid internal disruption by dispersing concentrations of disaffected workers to more rural environs.

**Long-Term Stability over Short-Term Growth**

According to the South China Morning Post, the impending economic crisis is rooted in expansive fiscal policy, increased government spending, rising property values, extremely lax monetary policies, record-high bank lending, and
exploitation of regulatory loopholes. In 2009, during the last economic crisis in China, then-Premier Wen Jiabao oversaw the disbursement of over $500 billion to stimulate the stagnating economy. This provided badly needed relief to the economy, but ongoing corruption and crony capitalism, combined with rising competition from lower-wage countries like Vietnam, ensured that growth continued to stagnate.

Between 2010 and 2015, Chinese economic growth steadily declined from 10.5% (annual GDP growth) to 6.9%, respectively. The current GDP growth target is 6.5%. Louis-Vincent Gave, co-founder of Gavekal Research, recently said “the 6.5% growth target, you can still achieve it, but at a higher and higher cost. So why would they want to keep doing that?” Gave added that the practice of dropping growth targets could serve to decrease short-term growth, but promote long-term sustainable growth.

Thus, this practice would align with Xi Jinping’s initiative to increase risk management capabilities. While increased oversight would impede short-term growth, it would offer a safety net to the overall economy, while structural reforms would ensure longer-term economic stability.
Saudi Corruption Crackdown Could Permanently Boost Oil Prices

The Middle East is heading for a major showdown if statements made by Saudi Crown Prince Mohammed bin Salman (MBS) and UAE’s minister of Foreign Affairs Gargash are to be taken literally.

Over the last couple of weeks, the Gulf region has been on a rollercoaster ride. Risk analysts are struggling to deal with the dramatically changing geopolitical and financial environment while a direct military confrontation between the Saudi-led alliance and Iran’s proxies is around the corner.

The signals coming from the Saudi capital Riyadh are still the same; Saudi Vision 2030 and the Aramco IPO are on track. The media remains skeptical about the unforeseen crackdown on corruption, a week after the so-called “Davos in the Desert” financial get-together in Riyadh (October 24-26), where 3,500 CEOs and financial wizards convened.

The fallout of the direct attack on Saudi Arabia’s financial moguls and construction giants, such as Prince Al-Waleed bin Talal and the Binladin Group, would put fear in the heads of investors in New York, London, Beijing, and Moscow.
Most agreed that bin Salman overplayed his hand, causing instability in the country and the region. The reality for insiders, however, looks different.

The anti-corruption crackdown by MBS is part of his overall strategy to implement Vision 2030. First of all, the Davos in the Desert meeting showed the financial world’s immense interest in investment opportunities in the kingdom. Considering that 99 percent of the attendees had never visited Saudi Arabia before, while only the speakers already represented a $22 trillion value of assets under management, MBS could tick off another box on his long list to make Vision 2030 a success.

At the same time, the Trump Administration and the UK government tried to woo MBS to list the Aramco IPO on their stock exchanges. Some would have become more lenient towards a flexible approach when looking at the amount of interest, but MBS upped the ante and pushed for new hard-needed changes. The anti-corruption crackdown was carefully considered and timely and served not only to remove corruption in the kingdom but can also be seen as a way to remove remaining opposition to MBS’s future reign. With military precision, MBS removed most of the obstacles still blocking a possible MSCI Emerging Markets Index listing in 2018.

By taking out high-profile businessmen that were already convicted several times for corruption and removing princes that held commanding positions within the armed forces, MBS moved the kingdom towards a more modern economy while consolidating his own power. The inclusion of the kingdom in the MSCI index will bring a multitude of FDI, much larger than the Aramco IPO. The MSCI Emerging Markets Index, for example, gives European pension and investment funds the possibility to invest in the kingdom and trade on its stock exchange. The Saudis have reportedly already attracted $9 billion in recent weeks. Some analysts are much more optimistic when looking at the long range of IPOs planned on the Tadawul (Saudi stock exchange).

MBS’s domestic popularity has increased in recent months. The Crown Prince has great support among the youth and has shown to be listening to the majority of his people while being unafraid to make dramatic changes to outdated social structures within the kingdom. Still, MBS understands internal Saudi politics and
will try not to completely upset the establishment.

At the same time, regional instability and unrest complicate MBS’s agenda. The confrontation between Arab nations and Iran has reached a tipping point. And looking at the statements made by UAE’s minister of foreign affairs on November 12 during the Emirates Policy Center’s Abu Dhabi Strategic Debates (ADSD2017) on Sky Arabia shocked the audience. The direct attack and accusations vented towards Iran and Qatar, both accused of promoting instability, financing terrorism, and extremism, were of an unprecedented tone. Gargash also accused both of committing “acts of war”, especially via arming Houthis in Yemen and Hezbollah. These accusations are openly supported and repeated by a long list of Arab politicians and leaders.

The war drums are being banged—and this time not as an empty threat, but as a precursor to real military action. Most analysts are looking to Riyadh, as they expect MBS to lead this operation against Lebanon’s Hezbollah and the Iranian IRGC; most likely the lead will be taken by the UAE.

Expect military action in the coming weeks, with—or without Washington’s support. The political show around Lebanese PM Hariri is only part of this. Analysts tend to forget that Hariri’s real power is in Saudi Arabia, where he is the owner of construction giant OGER, currently under investigation as it is in financial trouble. MBS has taken the opportunity to kill two birds with one stone and remove OGER out of the picture in Saudi Arabia while destabilizing Lebanon. This was organized in close cooperation with other Arab leaders. Sheikh Mohammed Bin Zayed, a close friend of MBS, will head the anti-IRGC venture, as Abu Dhabi has been doing for years under the radar in Yemen, Syria and especially Libya.

**Military action can be expected, with or without the support of Washington.**

As several Arab ministers and advisors have stated in recent days, it’s time for Arabs to take the future into their own hands. Washington can support, but not lead. If no American assistance is given, others will undoubtedly fill the gap. Moscow has been extremely quiet the last weeks, not indicating any support for Tehran nor trying to mitigate between the Riyadh-Abu Dhabi axis and
Iran-Hezbollah. These plans seem to have already been discussed in the respective capitals, as ministers of the said countries have convened in several places.

If action is taken against Iran and its proxies, OPEC and oil prices will be impacted immediately. Oil price increases of $5-10 per barrel a day could be a distinct possibility. An escalation in Lebanon, due to the inclusion of Israel in the action, or maritime traffic attacks in the Gulf, would only push prices up further. After years of low geopolitical risk premiums, risk has returned to the market.