Summary of Proceedings

Is Truth a Commodity?
Sovereignty in the Information Age

A është e vërteta një mall?

2018 Annual Conference
20-23 March 2018
Counterterrorism Fellowship Program
The Counterterrorism Fellowship Program (CTFP) is a United States Department of Defense program specifically designed to strengthen the capabilities of friendly countries to fight terrorism, as well as construct and strengthen the global network of experts and professionals who are dedicated to this fight.

USSOCOM appreciates the support of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict for the globally-recognized Sovereign Challenge Program.

Editors:
Gregory N. Hicks
Larry Cook

The United States Special Operations Command (USSOCOM) was activated in April 1987 to provide command, control and training for all Special Operations Forces (SOF) in the United States.

USSOCOM headquarters is at MacDill Air Force Base, FL. Its components include the U.S. Army Special Operations Command (USASOC), Fort Bragg, NC; the Air Force Special Operations Command (AFSOC), Hurlburt Field, FL; the Naval Special Warfare Command, (NSWC), Coronado, CA, and the Joint Special Operations Command (JSOC), Fort Bragg, NC.

SOF Truths
- Humans are more important than hardware
- Quality is better than quantity
- SOF cannot be mass produced
- Competent SOF cannot be created after emergencies occur
- Most Special Operations require non-SOF support
# TABLE OF CONTENTS

Conference Overview  
Towards a World Overview  
Three Decades of Innovative Crime Reduction and Counter-Terrorism Prevention  
Trust, Storytelling, and the 21st Century Media Environment  
Narrative Strategies and Narrative Warfare  
Technology, the Media, and the Degradation of Professional Journalism  
Russia’s Information Security Programs  
Flipping the Script – State and Non-State Actor Disinformation Efforts  
Countering Live and Virtual Terrorism with Increased Connectivity  
Message, Messenger, and Medium – Countering Disinformation Campaigns  
New York Harbor – A Focal Point of American History  
Technological Innovation, Innovators, Investors, and Responsibility  
Participant Perspectives  
Speaker Biographies
CONFERENCE OVERVIEW

United States Special Operations Command hosted the 2018 Sovereign Challenge annual conference, entitled, “Is Truth a Commodity? Sovereignty in the Information Age,” March 20-23 in New York City. Deception and disinformation in warfare are not new concepts. In fact, they have been primary military tenets since tactics and strategy were first conceived. But as with so many aspects of modern life, the rapid evolution and ubiquity of powerful new technologies have changed the ways in which deception and manipulation of information impact conflict. The technologies aren’t a threat in and of themselves, but they can be leveraged to amplify effects exponentially, creating greater complexity and wider consequence than heretofore experienced. Meanwhile, the democratization of technology has given individuals capabilities on par with corporations who have perhaps acquired capabilities that approach the purview of States. In this environment, critical thinking skills are vital for public resilience against disinformantion campaigns.

Keynote speaker Dr. Richard Haass, recalling key points from his new book, A World in Disarray, said that “[W]e live in a post-super power age. No single State has the concentrated power and ability to dominate, and ISIS, Al-Qaeda and others are showing that not all the players are States.” Microsoft Storyteller Steve Clayton and author Dr. Ajit Maan described the power of narratives, both true and false, to cement ideas in peoples’ minds. Both State competitors and non-State adversaries are effectively using “narrative warfare” to erode the trust of citizens in public institutions and to widen internal social, economic, and political divisions, and to magnify longstanding grievances with substantial effects. Counter-narratives and “fact-checking” are typically counterproductive. Instead, the more effective policy response is to craft positive narratives that resonate with intended audiences and align them among allies and partners. Finding the right message, messenger, and medium is the path to success, along with getting outside our echo chambers, our “policy bubbles,” and listening before turning on the transmit button.

Russian author Andrei Soldatov described President Putin’s deliberate erosion of Russian public trust in their government institutions to convince Russians to trust only him. His strategy is also to sow confusion and distrust in public institutions in the United States and Europe. Avoiding describing pro-Kremlin propaganda as “Russian” was important advice from East European speakers, along with effectively using humor, strengthening independent media, raising awareness among political leaders and populations, and raising the costs for using aggressive disinformation programming.

After receiving law enforcement and counter-terrorism briefings from the New York Police Department and FBI, participants heard a number of speakers address terrorist groups’ effective use of low cost technology and well-crafted, compelling narratives to mobilize resources, recruit people, and stimulate extreme violence across the globe. EUROPOL’s Deputy Executive Director of Operations, Mr. Wil van Gemert provided a comprehensive briefing on EUROPOL’s integrative role in countering online terrorist activity and supporting European law enforcement actions against terrorist groups. In Southeast Asia, empowering Muslim communities in religiously diverse cultures has been a key element in building social resilience to terrorist group messaging. Developing community-wide critical thinking skills and rebuilding ethical journalism are two fundamental elements to successful counter-terrorism information campaigns.

Finally, Maria Ressa, Marcel Granier, and Patience Zirima compellingly reminded us that repressive, authoritarian regimes are using these same narrative warfare tools to suppress freedom and democracy in their own countries. In Ressa’s view, “… the new gatekeepers, the social media platforms, have no rules except that of mob rule,” and dictators are weaponizing social media to whip up the mob against their political opponents. In addition to outright censorship, dictators and their cronies are flooding the market
with lies, alleging corruption and igniting sexual violence and misogyny to degrade political and media critics. The best answer has been to build broad international networks to support independent media, build positive narratives, and provide accurate information.

The conference featured over 100 participants, including 56 senior diplomatic, military, and security officials from 43 countries, of which 34 are currently hosting U.S. Special Operations Forces. Speakers at the event came from the Czech Republic, Denmark, The Netherlands, The Philippines, Russia, Singapore, Sweden, Ukraine, the United Kingdom, the United States, Venezuela, and Zimbabwe.

U.S. Special Operations Command and its Sovereign Challenge program thank the Atlantic Council for its support in recruiting speakers, coordinating the preparation of presentations, and drafting preparatory literature for the conference. These contributions were instrumental to the success of the event.

**Conference Participation**

**100 participants**
- Afghanistan
- Angola
- Armenia
- Australia
- Barbados
- Belgium
- Botswana
- Brazil
- Burkina Faso
- Cambodia
- Canada
- Chad
- Cote d’Ivoire
- Croatia
- Czech Republic
- Denmark
- Ecuador
- El Salvador
- Estonia
- France
- Gabon
- Georgia
- Germany
- Greece
- Guatemala
- Hungary
- Ireland
- Italy
- Kosovo
- Latvia
- Lithuania

**61 countries**
- Mali
- Mongolia
- Montenegro
- Netherlands
- New Zealand
- Nigeria
- Norway
- Oman
- Panama
- Paraguay
- Philippines
- Romania
- Russia
- Senegal
- Serbia
- Singapore
- Slovenia
- Sri Lanka
- Sudan
- Sweden
- Tanzania
- Thailand
- Uganda
- United Arab Emirates
- United Kingdom
- Ukraine
- Uruguay
- Venezuela
- Yemen
- Zimbabwe

* Not official government representatives
Council on Foreign Relations (CFR) President Dr. Richard Haass warmly welcomed to CFR’s headquarters the participants in the Sovereign Challenge Program’s 2018 annual conference. Dr. Haass observed that the international community is in the midst of the most challenging time since the post-World War II liberal order was established. Compared to now, the 40-year long Cold War was a relatively stable period of world history. In the 28 years since the end of the Cold War, the international system went from a bi-polar order to one in which power is distributed into more hands, making the international system more structurally difficult to regulate. Just as Voltaire observed that “the Holy Roman Empire was neither holy, nor Roman, nor an empire,” Haass questioned whether the post-World War II Liberal World Order remained liberal, global, or even an order.

This, Dr. Haass continued, is a highly stressed moment in history, where gaps between global objectives and international arrangements exist. We live in a post-super power age, he said. No single State has the concentrated power and ability to dominate, and ISIS, Al-Qaeda and others are showing that not all the players are States. All regions of the world are now much more dynamic and have the mark of instability. We have witnessed the return of geopolitics and great-power rivalry, as exemplified by Russia in Ukraine and China in the South China Sea; intra-state instability, which exists in Africa, the Middle East, and Latin America—where none of the states in those regions have adequate influence or power to maintain stability; and rogue regimes that are contesting the status quo, such as North Korea and Iran. Additionally, there is a rise of populism and nationalism that is contributing to democratic states becoming less democratic and authoritarian states becoming more authoritarian.

The Middle East, according to Dr. Haass, is an example of a subsystem that cannot manage itself and currently needs others to regulate it. Intra-state violence, proxy wars, and great power competition predominate, and there is no consensus on what the region ought to look like. Henry Kissinger had a formula that stated stability requires: (1) consensus of what the elements of stability should be comprised (e.g., clearly delineated borders, political legitimacy); and (2) force to deter challengers to it, or to assert force to defeat challengers that arise. Neither of these conditions currently exists in the Middle East, and it looks like we are only in the early days of this period of relative disorder.

We live in a world where much of what occurs inside the borders of another country is no longer its business alone, asserted Haass. Some governments, either out of choice or weakness, harbor terrorists or computer hackers. That is not solely the host government’s business, because a State is hosting people who have the ability to affect the prosperity and security of people everywhere.
Refugees, he continued, are another example in which sovereigns’ decisions affect the greater region or world. Venezuela is hemorrhaging people, and more than half the population of Syria is displaced, threatening the stability of its neighbors. Meanwhile, North Korea’s quest to develop nuclear weapons and a means to deliver them obviously affects people around the world.

Haass stressed that existing international institutions were not built to cope with the current rapidly changing environment characterized by the return of old competitions and the emergence of new challenges. For example, the cyber domain is a new “wild west” where very few rules exist with a very limited set of agreed enforcement options. Governments can no longer operate independently and expect success, but there is no consensus on the division of labor to tackle rapidly emerging problems. To have a lasting impact and improve stability in unstable areas, governments need to leverage allies and partners, as well as non-governmental organizations. As an example, Haass related, “the Secretary of the United Nations once asked me to get together a group of players in the world of global health, and I said, ‘... But we can’t just do it with the World Health Organization and member states of the UN.’ We had to bring in the Gates Foundation and pharmaceutical companies and so forth. We live in a world again where many more players are on many more chessboards. If I were to hand out pen and paper and ask you to design a U.N. Security Council, not one of you starting from scratch would design this Security Council with the United States, Russia, China, Britain and France having five permanent seats with vetoes and other countries not there.”

“We live in a world where much of what occurs inside the borders of another country is no longer its business alone. Some governments, either out of choice or weakness, harbor terrorists or computer hackers. And refugees are another example in which sovereigns’ decisions affect the greater region or world.” – Richard Haass

At the same time, Dr. Haass stated, the outsized influence that the United States enjoyed during the past 70 years is now changing. The United States, he said, will be more selective in what it does. Without the United States, the principal architect of the of the post-World War II order, the world will likely be less stable. Although not yet isolationist, for the foreseeable future the United States is unlikely to play the traditional role it once did in the liberal order. Therefore, what the U.S. signals it is, and is not, willing to do militarily (with North Korea, Venezuela, Syria, the South China Sea, and with Russia) will have major implications for international stability. Additionally, Haass suggested that other states cannot or will not fill the role that the United States appears to be vacating (China and Russia will not and European countries cannot). U.S. influence can be further undermined if allies and partners begin to doubt U.S. consistency, predictability, and reliability. Allies and partners will explore other options, and adversaries and competitors will doubt U.S. determination to use power, increasing risk across the globe.

Juxtaposed against the apparent trend of a decreasing international role for the United States, Haass reflected on China’s increasing strength and its meaning for global stability. For the last several decades, he noted, China has put its domestic and economic stability ahead of its foreign policy. Several changes, e.g., the end of term limits for Xi Jinping, rising military expenditures and China’s assertive regional behavior in the South and East China Seas, as well as towards Taiwan, signal that China may have altered its calculus, but China’s motives remain unclear. Some believe that China is becoming more nationalist for domestic political reasons, while others suggest China’s policy is opportunistic. Haas pointed out that debate is ongoing and the issue is likely to play out in unimaginable ways, but it is clear that a more assertive China could make for a very different 21st Century than previously imagined.
THREE DECADES OF INNOVATIVE CRIME REDUCTION AND COUNTER-TERRORISM PREVENTION

CHIEF DERMOT SHEA, NYPD AND ASSISTANT SPECIAL AGENT-IN-CHARGE CHARLES E. BERGER, FBI

Chief Dermot Shea of the New York Police Department’s (NYPD) Office of Crime Control Strategies provided conference participants with a comprehensive briefing on New York’s innovative strategies for reducing major crime in the United States’ largest city. Today, the NYPD employs over 61,000 persons including 36,000 police officers, 17,500 civilians, 3000 traffic officers, and 5000 school safety officers to maintain safety in an area of 304.6 square miles containing a population of eight and a half million people and including an additional two million daily commuters and one million tourists.

In 1990, New York City was a very dangerous place to live and work. In that year, over 700,000 crimes were reported, including over 2000 murders. The public viewed the NYPD as completely ineffective in fighting crime and corruption.

In response, the NYPD set realistic goals to reduce major crimes and improve public opinion about the force. Committing resources wisely, including heavy investments in technology, the NYPD focused on four main activities: 1) collection of accurate and timely intelligence 2) employment of effective tactics 3) rapid deployment and 4) relentless follow-up and assessment. The results have been remarkable. By 2017, major crimes had fallen to 96,517, and murders had decreased 87 percent to 292. However, while violent crime has decreased, white collar crime has increased and drug overdoses are becoming an increasing problem.

Effective use of technology and data to maximize scarce resources has been instrumental to the NYPD’s success. Over 100 new criminal analysts are sifting through incoming crime data, looking for trends to help focus resource allocations. An in-house NYPD tool known as the Domain Awareness System (DAS) tracks, sends automated alerts, and provides past, present, and trend information on targets (individuals, groups like gangs, and additional threats). The system, which is interoperable throughout the department and New York’s eight boroughs, uses multiple sources of data collection to create a site picture of the Area of Responsibility (AOR), ground activity, and a pattern of criminal activity. With DAS, police officers today have more information at their fingertips than ever before to assist in assessing criminal intent, activity, and to operate in a safer and better informed environment. Needless to say, the NYPD remains committed to research and development to stay ahead of threats.
Technology has also been enlisted to connect with communities and manage information and public relations. Media reporting is not always accurate. For instance, a recent report on a weapon in a school created a sense of public panic. However, the true story was that a student, who trusted a School Safety Officer, reported his own possession of a firearm and turned it in. In response, the NYPD is using social media and technology for outreach. In 2018, the NYPD conducted its first live stream of a community meeting to become more involved in community discussions and decisions.

Assistant Special Agent-in-Charge Charles E. Berger said that the FBI formed its first Joint Terrorism Task Force (JTTF) in 1980 to improve counter-terrorism collaboration and coordination between local, state, and federal law enforcement organizations. The FBI deputizes state and local law enforcement officers, like NYPD detectives, as U.S. Marshals to incorporate them into JTTFs. Since 2001, the JTTF concept has tripled in scale from 35 field offices to 103, and during a crisis, the FBI has the capability of forming a unified command across field offices. In addition, the JTTF has international responsibilities in Canada, Western Europe and Africa. At the request of a government, JTTFs can deploy to assist another State in a criminal investigation or other counter-terrorism-related law enforcement mission.

Tracking the strategic messaging of terrorist groups is a JTTF priority. One of the primary purposes of terrorists’ strategic messaging is competition between terrorist groups for relevancy, legitimacy, and prestige, but we are also seeing terrorist communications to attract future recruits, to inform existing followers, and to stimulate attacks. One pattern that worries us the most is messaging to stimulate homegrown terrorists by exploiting and widening domestic political divisions, because we have identified specific terrorist groups operating in the New York metropolitan area, especially in Queens, New York’s most ethnically diverse borough. As the JTTF tracks these groups, we are seeing their behavior rapidly adapt to our tactics, renting trucks to drive over pedestrians, or women traveling to terrorists’ bases to have jihadists’ babies. Nevertheless, the JTTF has seen some recent success in stopping homegrown terrorists from exiting the country to participate in overseas terrorist activities.
To illustrate the power of storytelling for the Sovereign Challenge audience, Microsoft Chief Storyteller Steve Clayton described his initial recruitment by Microsoft, which he summed up with the punchline; “... they hired the wrong Steve.” However, as these things do, Microsoft’s so-called “wrong” decision has enabled him and the company to define a needed role, because organizations across the globe are struggling with the crafting and sharing of their narratives in the current media environment. Storytelling, according to Clayton, is a comfortable and effective way to establish trust and to connect people to common values, shared interests, and relevant information in ways that audiences more easily assimilate. Clayton emphasized that people are not really wired to retain facts and data, but through storytelling, they can absorb key concepts and come together for common purposes.

The “2018 Edelman Trust Barometer” (http://cms.edelman.com), Clayton said, provides a useful set of analyses to help us better understand the current media environment. Edelman, he explained, developed the “Edelman Trust Barometer” to provide an annual report, based on public polling that measures trust in business, government, media, and non-governmental organizations.

According to the Edelman report, the “media” is seen around the globe as the least trusted institution in society. Again citing the Edelman study, the public defines “media” as both content and platform. More specifically, 89 percent sees the media as journalists, 48 percent see “media” as “social media,” and 40% actually see “media” as corporate brands. However, when asked to differentiate trust in “media” between journalism and platforms, the data indicated that public trust in journalists is increasing while trust in media platforms is falling. The study, Clayton continued, showed that half of people are “disengaged,” consuming news less than weekly. Another quarter consume news on a weekly basis or better, while the remainder actively consume and share news.

“What is going on in the world of media? Our platforms are under attack. Our profession is under attack. We have to act like we have an adversary in the media. We can’t just stand there on the field of play and pretend that there isn’t an adversary who is actually trying to use our platforms, who is trying to undermine the trust that we’ve built in our technology, undermine the trust in the media.” – Steve Clayton
Declining trust in “media,” Clayton suggested, relates directly to public perceptions about the reliability of information that media platforms are making available to the public, and this relates directly to the spread of false narratives. Seven of ten people in the United States are worried about fake news being used as a weapon. Media companies, Clayton emphasized, are chasing “sensational” news and consumer clicks to generate revenue. Both Facebook and Google are very much built on revenue generated from the advertising business, but they are not alone. For many of the technological products that we use, if they are obtained for “free,” then the consumer is the product, because his or her identity is being monetized through advertising. It should come as no surprise that trust in the media has fallen the most in the United States. On the other hand, trust in the media is actually rising in places like China and India.

“Getting outside our ‘bubbles,’ our closed circles of contacts and regular information sources that reinforce our own assumptions and analysis, is essential to activating our own critical thinking skills, while setting a positive example for others.” – Steve Clayton

Meanwhile, trust in business leaders and businesses has been increasing. Observing these trends and recognizing that Microsoft’s own narratives were not being told by established media, the company decided to begin telling its own stories to promote its own narratives about the company’s purpose and objectives. Clayton suggested that others may wish to follow Microsoft’s lead; “now, we all have a job to spread the narrative of our organizations and governments as amplifiers.” However, Clayton cautioned that businesses in particular need to present themselves as committed to the long term systemic health of their respective political/economic systems, and not just short term profits.

Because many people appear not to have the skills to verify the information they are consuming, all of us, Clayton urged, will need to raise our own critical thinking skills and help others do the same. “Getting outside our ‘bubbles,’ our closed circles of contacts and regular information sources that reinforce our own assumptions and analysis, is essential to activating our own critical thinking skills, while setting a positive example for others,” he recommended. Likewise, he continued, we should minimize the spread of “fake news viruses” by refraining from rehashing or clarifying such stories, including from commentary on web posts and/or turning them off entirely.

Additionally, Clayton suggested that people should begin turning the current tech business model upside down. Instead of giving away the personal data that internet media platforms monetize through advertising, Clayton suggested that individuals could auction their own information for limited periods to specific companies, and instead of the tech companies getting paid, the individual would be compensated directly for their information. Just this small change could have dramatic impacts on both the technology and media sectors, he urged.

Finally, Clayton cautioned the audience by quoting Kevin Plank, the CEO of Under Armour - “Trust is earned in drops and lost in buckets.” The quote, he said, is on the wall of his office and imbues every aspect of his and his team’s work. “One single act,” he stressed, “can shatter that trust,” so we need to act accordingly as we tell our own stories and work with media.
“Why can’t we effectively counter disinformation with truth?” asked Dr. Maan. The “human dimension answer” to this question, Maan explained, is that information provided to people as raw data is not as influential as compelling stories. There is a cognitive biological/neuroscience answer to this: imaging shows that the human brain is more receptive to information that is delivered in story form. The ancients knew this intuitively, as was reflected by the stories they told. For example, The Illiad by Homer, though a myth, was still a narrative that resonates with western societies. Narratives like this help humans frame their own stories.

Maan emphasized that just because a narrative or story is not true does not make it less meaningful. If disinformation is told better than the truth, falsehood has greater impact. Effective narratives consist of three elements: (1) the meaning of the information (meaning of truth and lies); (2) the identity of the audience (cultural relevance to the audience it is targeting); and (3) a contextualized format that is familiar to the listener (ties information together into story form). Additionally, a storyteller will be most effective if her narrative addresses all layers of personal identity – from personal, to family, to national, and higher.

“Contemporary wars,” Maan explained, “are influence wars, and influence wars are not necessarily won by those with the most accurate information or the most recent information. They are won by people who can effectively tell an audience what the information means and what it means specifically for them. Just as the power of myths and stories and narratives does not rely on truth or facts or the accuracy of information for its effectiveness, so too, if disinformation is narrated, storified, mythologized, it will give people a way to understand their experiences that is, in fact, impervious to the truth. That’s the human dimension of the commodification of truth.”

Some States and non-state actors are exploiting and leveraging media uncertainty, domestic disagreements and pre-existing hostilities. When narratives are weaponized, they can impact domestic and regional security, shake the rule of law, cause civil unrest, and be a very effective tool for extremist recruiters and for radicalization. Narratives are power-shifting and the United States, along with allies and partners need to get into the fight. For example, ISIS starts with a narrative and conducts operations that tell a story. Additionally, AQ and now ISIS falsely tie the response against violent extremism to an attack of all of Islam. Eliminating terrorists is only a short-term fix; we need to make terrorist narratives obsolete. This is not information warfare, it is narrative warfare.
We need to meet weaponized narratives with a comprehensive narrative strategy. “I’m not talking about information warfare, as people often do. This is warfare over the meaning of information. It’s narrative warfare, which is a different thing,” she emphasized. Our strategy, according to Maan, should not focus around counter-narrative, but rather the United States, allies, and partners need to get better at telling our story; telling the world what we are doing, where we are doing it and why (and this needs to gel with what we are saying domestically). It should consist of a group of stories that show an international community banded together for the collective peace of nations. The credibility of the narrator, she stressed, is imperative; civilians or non-governmental organizations (instead of the military) should be the storytellers.

In Maan’s view, the central narrative of stories needs to work in different environments without conflicting or contradicting. One narrative level is insufficient for a strategy. We need strategic, meta (narratives about narratives), and tactical narratives that both influence domestic and international communities and exploit contradictions between the walk and talk of adversaries. To craft successful narratives, she highlighted, we must better understand the content, structures, and forms that best resonate with target audiences.

Going forward, Maan recommends shifting resources from counter-narrative efforts. “To the extent that truth telling is part of our strategy, it can’t be reactive. We can’t chase our adversaries around, matching their lies with our truth, because as cognitive science has demonstrated “… repeating lies with the word no or some other negative in front of them actually reiterates and strengthens those lies in the mind of the audience ...,” she explained. Instead, gathering information to understand the environment is a much more important component of narrative crafting. The United States, for example, does not need a single narrative, but American narratives just need to be harmonious. If the United States uses the Bill of Rights and Constitution as the basis of its narratives, debate and disagreement (which are fundamentally part of an American democracy that values freedom) can exist, as long as all narratives are anchored in those documents.

In conclusion, Dr. Maan reiterated that we need to improve our own stories and our own storytellers, while plugging some glaring credibility gaps. Our adversaries exploit obvious hypocrisies in our stories, she reminded. It is not enough to have an “influence containment” strategy. We need an improved cooperative strategy among allies and partners that will erode the will of adversaries, contain their influence, and dominate the narrative space. Ways and means need to be focused towards this purpose. Additionally, end-states will not look the same as a conventional fight, there will not be any clear winner. The competition, she highlighted, is perpetual.

“If disinformation is narrated, storied, mythologized, it will give people a way to understand their experiences that is, in fact, impervious to the truth. That’s the human dimension of the commodification of truth.” – Ajit Maan
Over the last twenty years, technology has drastically altered the global media landscape, deleteriously in many circumstances, according to all three panelists. Technology, asserted Ressa, has atomized everything to meaninglessness. Everything is hyper-charged with emotion. Social media is about thinking fast, but if you are thinking slowly, it just won’t spread. Established news organizations, Braw added, are operating at a disadvantage because real news is just not as juicy as the falsehoods that are being spread to confuse the public and make the public lose trust in traditional news organizations. Professional journalists, Ressa lamented, are no longer the gatekeepers. And the new gatekeepers, the social media platforms, have no rules except that of mob rule.

In Europe, disinformation associated with Russian-linked media outlets is pervasive, said Braw. One campaign featured a decades-old photo of American soldiers buying alcohol in a German supermarket, but the caption said that NATO soldiers were buying up all the alcohol in Latvia. How, Braw asked, can an ordinary citizen of Latvia, Lithuania, or Poland determine the veracity of the news item? As important for policymakers, she continued, any soldier serving in another country has become a target for hostile disinformation campaigns. More broadly, companies’ share prices are being negatively affected by political disinformation campaigns, despite their having nothing to do with the companies themselves.

The Philippines, said Ressa, one of Southeast Asia’s thriving democracies, has in less than eighteen months experienced a dramatic swing in its media environment. Filipinos, she continued, spend the highest amount of time online in the world, and as of January 2018, Filipinos spend the most time on social media. “In fact, our public space is Facebook. That is where democracy is created and discussed,” she said. However, soon after President Duterte was elected, the nature of this space began to change as social media was progressively weaponized against the president’s critics.

The first targets on Facebook were the people who questioned the drug war, followed by the journalists, both individually and news organizations, and finally opposition politicians. Paid trolls, fallacious reasoning, leaps in logic, and poisoning the well are preferred tactics. Instead of censoring, Duterte’s cronies and others like them are flooding the market with lies, drowning the truth. They are systematically attacking the credibility of opponents, first alleging corruption and repeating the allegations exponentially. Sexual violence, designed to inflame biases, fuel misogyny, and degrade the opponent as a sexual object, follows. Both former Philippines Secretary of Justice Leila de Lima and Ressa have been subjected to such abuse, both culminating in #ArrestLeila and #ArrestMariaResser Twitter and Facebook campaigns.

Tracking this phenomenon, Rappler identified a number of fake Facebook accounts and analyzed their activity, she briefed. One account used the internet photo of a Korean popstar. Connected to 26 Facebook friends, everything this group said on the Facebook pages was a lie, but over three months of communications that peaked at 90 hate messages per hour, these 26 individuals reached three million people. This is manufactured reality, she stressed.

Significantly, campaigns like this one are demographically segmented. Separate accounts target the masses,
others speak to the middle class, and another is “pseudointellec
tual,” she continued. The latter, she said, is a columnis
t at The Manila Times, whose owner handles Duterte’s interna
tional public relations. Even the head of social media communi
cations for the presidential palace is involved, she added.

“Established news organizations are operating at a disad
vantage because real news is just not as juicy as the falsehoods that are being spread to confuse the public and make the public lose trust in traditional news organizations.” – Elisabeth Braw

Venezuela’s independent media has suffered near constant persecution from the Chavez and Maduro governments, but the changes have taken place over nearly two decades, related Marcel Granier. When the media began reporting corruption in the PDVSA (Venezuela’s national oil company) and the military, along with their involvement in drug trafficking, Chavez began attacking journalists. After he revoked the licenses for local broadcast media, some turned to cable and satellite broadcasting, expanding market penetration from 20 percent to 70 percent. Chavez retaliated again, bribing cable and satellite operators to take critical channels off the air. Our internet sites were also blocked, he related.

Little by little, Chavez and Maduro have been eliminating the free press, Granier explained. Of the three largest newspapers in Venezuela, two of them have been bought by friends of the government, and the third one has seen its circulation fall from 150,000 copies per day to 7,000 copies per day. Instead of comprising between 64 and 128 pages per day, they have been reduced to between 8 and 16 pages. Most journalists have left the country because they cannot make a living in Venezuela, Granier added.

Chavez achieved his goals, Granier clarified, by daily expropriating three hours and 20 minutes of every station’s air time to line up his enemy du jour – landowners, entrepreneurs, foreign business, independent media, and the United States – and discredit them with the public. When Chavez took power, two-thirds of Venezuelans viewed the United States favorably and 5 percent thought highly of Cuba. Today, Granier related, Cuba controls the Venezuelan government’s information services and personal identity operations. The influence of Cuba’s and Venezuela’s special friends, Russia and China, is growing throughout Latin America, and the drug trade, which is controlled by Venezuela’s military, runs through the Venezuelan state of Apure. Corruption, Granier said, facilitated through Venezuelan construction companies and the state oil company, is being used to buy elections in El Salvador, Nicaragua, Guatemala, Honduras, Colombia, Ecuador, and Peru. Meanwhile, Venezuela’s independent media, which has been reporting all of these developments for two decades, is being ignored while it is slowly choked out of existence.

There are no easy answers to these dilemmas, Ressa commented. The platforms need to realize that in the virtual polities they have created, their algorithms have effectively nullified existing laws, leaving only the law of the mob governing virtual reality. The mob, she continued, has always followed popularity, and facts have never been popular. Moreover, there is no accountability in the virtual world, she stressed. Both governments and the platforms have impunity and the platform leaders do not care. In a 2017 meeting with Facebook’s Mark Zuckerberg, Ressa said that she explained how Facebook is being used in The Philippines, but the only thing that caught his attention from my presentation was the 97 percent Facebook penetration in The Philippines. He asked, “What are the other three percent doing?”

“Professional journalists are no longer the gatekeepers. And the new gatekeepers, the social media platforms, have no rules except that of mob rule. The mob has always followed popularity, and facts have never been popular.” – Maria Ressa

However, Granier cautioned that it is too easy to make Facebook and Twitter the villains of these developments, when the real scoundrels are the Chavez’s and Putin’s of the world. In his case, when Chavez branded his station as thieves, criminals, murderers, rapists, and worse, Wikipedia, Facebook, Twitter, and YouTube all responded favorably to the argument that Chavez and his cronies were in fact thieves stealing their property rights.
Russia as a society, explained Andrei Soldatov, co-author of The Red Web: The Struggle Between Russia’s Digital Dictators and The New Online Revolutionaries, is more than a bit conspiratorial and paranoid, and this affects senior level decision making. People in the Kremlin are trained to see the world in terms of threats to the stability of the political regime in Russia. Thus, every crisis in the world, regardless of geography, is seen as a potential threat to Russia’s political stability. For example, when Robert Mugabe was forced to step down in Zimbabwe, there was a huge outcry in the Russian media; the very idea that someone could be forced into stepping down was considered to be a threat to Russia’s leadership and system.

After the collapse of the Soviet Empire, the West assumed the Cold War was over, but, as Soldatov related, Russians never believed that the Cold War really ended – particularly in Information Operations. During the Soviet era, KGB-run externally focused disinformation operations were known as Active Measures. When the U.S. politely asked Russia to stop conducting Active Measures in the United States, Russia simply changed the name to “Assistance Programs” and never changed the methods, structure, and employees associated with Active Measures.

During the first Chechen war, from 1994-1996, the Kremlin believed that journalists actively undermined its war efforts. In 1999, during the Second Chechen War, Russia realized two things: 1) it was engaged in an information war, and 2) it was losing the war. In light of this Russia developed a new “Information Security” doctrine, which is much broader than the corresponding Western construct of Cyber Security. Russian authorities feel a need to control content, not just secure the method of transmission. During the Kremlin’s extensive efforts to control the story related to the Second Chechen War, the Chechen separatists countered by starting their own websites on foreign servers, and Russian government efforts to shut down the sites were far from successful.

“Putin’s message to the Russian people is that everyone in Russian politics is corrupt and only he can be trusted. Thus, a confused population chose the strong leader in the March elections, “… because there is no one else. Nobody trusts anybody. Nobody trusts the trade unions. Nobody trusts journalists. Nobody trusts any institutions like parliament.”
– Andrei Soldatov

On the other hand, Russia’s leaders noticed some strange behavior during this period. Online student groups, some of them based in Siberia, were successfully attacking Chechen websites on their own. Russia’s security services immediately latched on to these independent hackers and enjoyed two distinct benefits from the relationship: 1) it provided the Kremlin with plausible deniability, and 2)
the independent hackers were far superior to state-run efforts. Russia’s ability to harness these proxy hackers was directly responsible for a dramatic change in the scope, scale, and methods of its information security program, yielding the current new and improved version of Active Measures.

During the Soviet era, Active Measures and the KGB department that conducted them were strictly focused externally. There was an unbreachable firewall separating domestic security operations and Active Measures. After the success of the hacker proxies against Chechnya, President Putin, in one of his first acts, tore down this wall. Significantly, the document that effected the change declared that foreign media posed a threat to Russia’s information security.

For the very first time in Russian history, the same people were conducting information domain activities inside the country and outside. For example, the same group (Fancy Bear) that hacked the US Democratic National Committee was concurrently attacking Russian independent journalists based in Moscow.

The impacts of these changes have been consequential, Soldatov argued. Inside Russia, Putin has been deliberately eroding the institutions of government. The foreign ministry, according to Soldatov, no longer defines Russian foreign policy. That function now takes place within the administration of the president, and everyone knows that speaking to Foreign Minister Lavrov about Ukraine or Syria is a waste of time.

More broadly, Putin has jailed five regional governors, a Minister of Economic Development, theater directors, political activists, and ordinary people. “Last year, was the very first time in my memory that the general of the FSB (Russia’s security service) was sent to jail,” he said. Putin’s message to the Russian people, Soldatov continued, is that everyone in Russian politics is corrupt and only he can be trusted. Thus, a confused population chose the strong leader in the March elections, “… because there is no one else. Nobody trusts anybody. Nobody trusts the trade unions. Nobody trusts journalists. Nobody trusts any institutions like parliament,” he said.

Externally, Putin’s strategy is to give the West the same gift, to sow the same confusion, the same climate of distrust within America and Europe’s democracies that exists within Russia. In some places, like Ukraine, Russian misinformation campaigns have been highly successfully, because they are carefully tailored to preconceived biases and exploit longstanding mistrust. While Putin did not create environment(s) of mistrust, he has become an expert at exploiting social division and suspicion.

Countering Putin’s strategy, Soldatov suggested, requires understanding that Putin is a highly emotional individual who deeply wants to return Russia to equal status with the United States, and that he personally wants to be treated as the equal of the President of the United States. These emotions, Soldatov continued, are shared by many Russians. Putin’s legitimacy and popularity in the country are tightly connected with the confrontation with the West. He relies on confrontation, and when he thinks that he is losing his popularity, his first thought is to use an existing confrontation or create a new one, e.g., Chechnya, the Belgrade bombing, Georgia, Libya, Crimea, Ukraine, even Skripal. Thus, identifying inconsistencies in Russian narratives may be somewhat effective, although they carry the risk of increasing Putin’s popularity. A better approach would be to rely on positive Western narratives.
According to Zahed Amanallah of the Institute for Strategic Dialogue, the counter-extremism community vastly underestimated the impact of ISIS’ propaganda and disinformation strategies. The group effectively exploited the exponential technical power of globally connected, low-cost hardware and software to distribute well-crafted, compelling narratives to audiences around the world. Coming closest among terrorist groups to mimicking State actor information capabilities, these messages attracted thousands to leave their homes and go to Syria. “Ten years ago, you would have thought this would be impossible,” Amanallah said.

There is, Amanallah continued, an identifiable nexus between State and non-State actor disinformation efforts during political elections with extremist activity spiking and State actors seeking to exploit that effect. For instance, we have seen trolls collecting a Muslim-American group and trying to pit them against far-right factions. In the recent German elections, both bots and trolls sourced in Russia and far right groups from outside Germany attempted to influence the outcome. Similarly, in Kenya, Al-Shabaab tried to work tribal and religious fault lines during the 2017 elections to divide Kenyan society and create political instability.

In Ukraine, the problem of State and non-State actor disinformation efforts to affect public opinion emerged in 2013, when Ukrainians began demonstrating to support a free trade agreement with the European Union, according to Yarema Dukh, former Special Assistant to the Press Secretary of the President of Ukraine. The following year, Dukh continued, saw Russia’s annexation of Crimea, aggression in Ukraine, and a flood of false narratives, including the portrayal of Ukrainian patriots as Nazis, attempts to define Ukraine as perpetually a part of Russia, impersonation of senior Ukrainian officials in interviews with western media forums, as well as Russia’s allied trolls, pranksters, and on-line communities, and others. The amount of information was so large, that determining truth or falsehood was extremely difficult, and “fact-checking” efforts simply could not keep up with new stories appearing so fast that they left the “fact-checkers” in the dust.

I was surprised when a New York Times journalist called to clarify some statements that President Poroshenko had made in his previous interview, because I knew of no such interview and neither did the president’s press secretary. As we delved into the story, we learned that the New York Times received a message from poroshenkopress@gmail.com offering an interview, and the interview was held by telephone with a Russian translator. This should have been a red flag, because President Poroshenko speaks English on a very high level. Fortunately, the New York Times reporter’s follow up prevented the publication of a hoax, and recognizing its mistake, the New York Times posted the true story, which can still be found on the website. – Yarema Dukh
Noting that the problem of disinformation and propaganda has become a global phenomenon, Ukrainian journalist Maxim Eristavi posited that a crisis within the media profession is magnifying the problem. The past two decades have witnessed substantial staff reductions in existing media companies; meanwhile, the quality of journalists has also fallen. Organized mass disinformation is being disguised as news, and it is successful because people feel good about what they read. Eristavi expressed dismay about the numbers of Western journalists constantly asking questions in Kyiv like “Are Ukrainians Nazis?” or “Is the Ukrainian government a Nazi government?,” clearly indicating that they had already subscribed to Russian propaganda. In effect, weak journalism on the ground in Eastern Europe, whether local or international, could not cope with the high-quality content disseminated by the neighboring state’s very well-financed, well-oiled propaganda machine. Consequently, public confidence in journalists and the media industry has plummeted, he concluded.

“\textit{The volume of Russian information flooding Ukraine was so large, that determining truth or falsehood was extremely difficult, and “fact-checking” efforts simply could not keep up with new stories appearing so fast that they left the fact-checkers in the dust.”} – Yarema Dukh

As representatives of government, journalism, and the NGO community, each presented a different perspective on means to address these problem sets, but they also agreed on much. Amanallah stressed that every individual has a narrative. One way to build public resilience to false narratives is the development of a national narrative that is both derived from and embedded in the stories of individuals across the country. Instilling better critical thinking skills among the population, offered Eristavi and Dukh, would also strengthen public resilience to false narratives. Together, they would enable citizens to escape the natural filter bubbles of their “tribes,” which broadcasters of false narratives seek to exploit.

All three agreed that social media was both a problem and part of a solution to the problem. Dukh related that both Twitter and Facebook had been important partners for countering Russian propaganda, not only as platforms for Ukraine’s positive information programming that reached millions of viewers, but also as verifiers of Ukraine’s official accounts. On the other hand, Amanallah cautioned that Facebook’s Artificial Intelligence that was designed to identify extremist narratives and posts has been largely unsuccessful. For his part, panel moderator John Watts suggested that the use of GIFs, Emojis, and Memes provides important context for messaging that would otherwise not be present, helping to distill complex ideas into more compact and understandable forms. Ukraine, Watts noted, was particularly successful with these techniques.

All the participants stressed the importance of using proper terminology. “Fake news,” they said, actually harms journalists and journalism by making the term “news” a negative value. Similarly, Dukh and Eristavi strongly recommended minimization of the term Russia or Russians when discussing disinformation emanating from that country. Using these terms feeds Putin’s internal propaganda and xenophobia, strengthening his political base. Instead, both argued that disinformation emanating from Russia should be identified as Putin’s or the Kremlin’s propaganda.

Ultimately, Eristavi said, we all need to support “making journalism, and especially independent journalism, great again.” No matter where they live, people are starved for brief, accurate reporting that provides valuable context. “Journalism is about telling the truth,” he concluded.
Since 2015, Europe has suffered from an increasing number of Jihadist attacks that have also been dramatically changing in nature, stated Mr. van Gemert. Perpetrators are increasingly diversified, ranging from radicalized youth to lone actors not directly associated with any particular Jihadi group. Some perpetrators had returned from conflict zones, but others had resided in Europe for a long period and never been anywhere near a conflict zone. Modus operandi have also diversified between apparently unplanned, indiscriminate killings such as the truck driver in Nice and well-prepared attacks like those in Paris, Brussels, Manchester, and Barcelona, he said.

Other patterns have emerged. A substantial number of the perpetrators were known to the police but not considered an immediate terrorist threat towards European society. All of the attacks seem to be connected to each other in some way. Many were attacks on symbols of Western lifestyle that Jihadists see as morally corrupt, such as concert venues and nightclubs. Others were symbols of Western authority like the attacks on police and military service members in France.

The evolution of the European terrorist threat environment is closely linked to the three phases of the rise and fall of the so-called Islamic State. Phase one saw a major flow of European fighters to Middle Eastern conflict zones and attacks coordinated by ISIS in Paris and Brussels. During phase two, European governments actively prevented and disrupted travel to conflict zones, leading to smaller scale attacks by home-grown, radicals. As ISIS contracted, it altered its propaganda to encourage radicalized Europeans to launch attacks wherever they live with whatever tools are available, leading to attacks in France, Belgium, and Germany with weapons including rented vehicles, knives, machetes, and improvised explosive devices.

A central characteristic associated with the ISIS campaign in Europe has been the intense and professional use of social media for communication, radicalization, and recruitment. They have not only shown extremely skillful use of technology but also innovative flexibility in their reaction to European governments’ countermoves.” Wil van Gemert

A central characteristic associated with the ISIS campaign in Europe has been the intense and professional use of social media for communication, radicalization, and recruitment. They have not only shown extremely skillful use of technology but also innovative flexibility in their reaction to European governments’ countermoves. Under pressure, they have shifted their communications across social media, web pages, blogs and smaller and smaller platforms and forms that had not been seen before and were difficult to identify and reach by governments and law enforcement. As they varied their use of platforms, ISIS also transformed its narratives from inviting believers to come fight in conflict zones to calling for attacks in countries of residence while also seeking to expand the group’s influence within Europe’s Muslim communities. They have even turned to recommending that young Muslims join Europe’s military forces to use that knowledge in the future.

The European Union has 500 million inhabitants and two million law enforcement officers, and EUROPOL’s purpose is to support them in a broad range of activities. EUROPOL’s core function is
to gather data from member state national police investigations and add value to them by making connections between similar ongoing investigations in other member states or adding extra relevant information from other sources. To accomplish its counter terrorism mission, EUROPOL’s Operations Directorate employs over 100 individuals and has compiled a database of 500,000 entities and 40,000 individuals that have some relation to terrorism. With these resources, EUROPOL supported over 400 law enforcement counter terrorism operations over the past two years.

To counter ISIS’s and other terrorist groups strategic use of the internet, Europe’s justice ministers asked EUROPOL to establish an Internet Referral Unit (IRU) to identify illegal internet content related to terrorism and to provide additional support to criminal terrorism investigations. Currently, twenty employees work in the IRU to flag extremist internet content and work with industry to remove that content from the net. Since the beginning of 2015, the IRU identified 45,000 internet items that contained violent content or encouraged commission of violent acts on over 70 internet platforms, of which we convinced the providers to take down 85 percent. This success relates directly to the public-private partnership relationships we are building and strengthening with industry.

Looking ahead, EUROPOL is transitioning from an information collecting organization, with databases containing information on more than 100 million organizations related to thirty forms of organized crime and terrorism, to an organization that connects international law enforcement, national law enforcement, industry, and other relevant groups to each other and with relevant information. In recognition of this potential, we now have 44 countries represented at EUROPOL headquarters, including the United States, which alone has 26 liaison officers assigned to EUROPOL. These relationships are also facilitating EUROPOL’s ability to support transnational criminal investigations of both terrorist acts and organized crime, including through EUROPOL’s fielding of joint investigation teams composed of representatives from multiple countries.
“Every living room,” Farwell began, “and every cell phone has become a battle space.” It is widely recognized, he continued, that information warfare, information strategy, and strategic communication can determine the outcome of international competition between state actors or between state and non-state actors, just as surely as kinetic operations. Our adversaries have learned this and they are effectively employing tactical information operations to create strategic effects.

Advertising, Farewell related, is part of the lifeblood of commerce in democratic/capitalist societies, but our less-sophisticated adversaries are proving more adept, more agile, more flexible and imaginative information warriors. ISIS information operations have persuaded, recruited, and mobilized people all over the world to overthrow regimes ISIS views as apostate and to establish a global caliphate. Russia has shown extraordinary sophistication, and they have put the resources behind it, in both the United States and in Europe, to conduct information operations aimed at sowing chaos and discord, inflaming emotions, and widening the divisions of already polarized electorates. They are maximizing the key precept of information warfare: reason only persuades, but emotion motivates behavior.

According to Patience Zirima, the political context in Zimbabwe appears to be changing, but perhaps for the better. Since the November 2017 elections, Zimbabweans have some hope that the highly repressive, authoritarian regime that has ruled for the last 20 years is on its way out. Despite this repressive environment, which nearly extinguished independent media in the country, Zimbabwe has become part of the global village. Internet penetration has grown exponentially, as many as 90 percent of Zimbabweans are online, mostly using WhatsApp.

Zirima’s organization, Media Monitors Zimbabwe, tracks the mainstream media, WhatsApp, Facebook, Twitter, and other sources. For instance, the ruling party has built its own Twitter team to attack the opposition, who are also creating content. Even Russian groups have been intervening in our domestic political debates, she commented.

It is clear, said Zirima, that responses to disinformation, to fake news, cannot be one dimensional. They must be holistic, so we have tried to build a broad, international network of organizations – e.g., youth groups, women’s groups, and regional media organizations – who are working together to counter disinformation by promoting the growth of independent media that provide accurate information. To support these efforts, Media Monitors Zimbabwe’s fact-checking program, ZimCheck, is designed to hold the press, both independent and state-owned, accountable for the material they present.

Agreeing with Zirima, Singapore’s Susan Sim said that there is no one size fits all model for countering disinformation or, as Singapore is learning to call it, online falsehoods. Thus, Singapore’s counter-terrorism strategy is based on the premise that society must be resilient to radical rhetoric, because both ISIS and Al-Qaeda rely on deliberate misinterpretation and misuse of religious concepts to justify their violence and to influence people to support their cause.

Disinformation works by attacking fault lines, by feeding into community biases, Sim continued. Jihadist narratives reinforce community differentiation, seeking to isolate groups based on religious and ethnic differences. They frame false choices such as “I want to live a noble life or die a martyr.” They are designed, in many ways, to exploit online echo chambers where people hear what they want to hear, and if their ideas are challenged, they become even more entrenched.

For Singapore, credibility and effectiveness lies in getting the message, the messenger, and the medium right, Sim asserted.
Thus, Singapore chose to empower the community at risk to deal with this existential threat to the most religiously diverse country in the world. Singapore’s Muslim leaders use their knowledge and expertise to help rehabilitate terrorists who have been detained, to counsel the family members of those who have been detained, and to educate the public at large about how al Qaeda and now ISIS have distorted Islamic beliefs. Instead of Muslims in Singapore believing they are a community under siege, they stand proudly and say, “We are Singaporeans, and we are doing everything we can to secure our country.” And the results speak for themselves. They have helped to rehabilitate 88 percent of those Singapore has detained for terrorism.

In this, the idea of second chances has been very powerful, but the political will to act against recidivist criminals is equally important, Sim stressed. Jail must be a real threat, but you must also develop an engaged citizenry that is willing to stand up for its beliefs and its values, as well as support legislation to provide deterrence mechanisms. What we are talking about is developing community-wide critical thinking skills that inoculate society against disinformation and terrorism, Sim concluded.

To challenge pro-Kremlin disinformation campaigns, related Jakub Kalensky, the EU has three priorities – promoting EU policies in the eastern partnership countries: Belarus, Ukraine, Moldova, and the three Caucasus Republics; supporting the region’s independent media; and raising awareness about Putin’s propaganda. If Georgians understand that the EU is about building roads and hospitals, Kalensky stated, if they are aware that Sputnik Georgia’s stories that the EU is trying to turn Georgians into gays and pedophiles are part of an orchestrated disinformation campaign, and if Georgia has a stronger, independent media environment, Georgians and others will prove to be more resilient to pro-Kremlin disinformation.

Initially, the EU’s East StratCom Task Force had no budget, Kalensky stressed, so cooperation with frontline state partners – first, Ukraine, Estonia, Latvia, and Lithuania, then Sweden and Finland – was essential. We have learned a great deal from their experiences coping with pro-Kremlin disinformation. Lithuanian Army StratCom has been truly amazing. They identified a false narrative, and before it was released, briefed political leaders, key government officials, and the media, effectively inoculating the people against a false belief that was about to be implanted. In so doing, they obviated the need to undertake one of the most difficult information warfare tasks – convincing people after the fact that they have adopted a false belief.

Working with our front-line partners, Kalensky outlined, we have developed a five-step course of action for countering pro-Kremlin disinformation campaigns. First, countries should expand their level of awareness with 24/7 monitoring of the information space and understanding the social, cultural, and economic vulnerabilities – e.g., Russian-speaking minorities or concentrations of unemployed youth – that pro-Kremlin disinformation might seek to exploit.

Second, political leaders must actively raise public awareness. When Angela Merkel and Emmanuel Macron addressed pro-Kremlin propaganda and election meddling, the public listened, but more must be done, he stressed. The American election meddling investigations are an example that Europe, especially after obvious Putinesque interference in the French and Czech presidential elections, as well Germany’s parliamentary elections, needs to follow, Kalensky recommended.

Disinformation works, stressed Kalensky, by misleading people. However, they do not like to be misled. Ukraine’s StopFake.org has no peer in revealing and documenting the organization and activities of the disinformation machine, step three in combating it. By exposing disinformation to the people, day in and day out, Kalensky emphasized, they are better prepared, inoculated so to speak, to resist the next disinformation effort.

As Yarema Dukh highlighted in his comments, humor can be a powerful tool to counter Putin’s disinformation machine, Kalensky highlighted. Ridiculing the machine is something that can actually reach other audiences, even experts, mused Kalensky. The twitter account @DarthPutinKGB, he suggested, perhaps best exemplifies this fourth element to an effective counter-disinformation campaign, but ridicule is probably a tool that government should eschew in favor of civil society and media, he recommended.

The fifth element, Kalensky concluded, is a careful identification of tools that raise the costs for the Kremlin to conduct these operations. Like our approach to espionage, we know that we will never eradicate spying, but we can make it more expensive.

Responding to a question from the floor, Sim, a former journalist, recalled that responsible journalism requires a balance between breaking the story first and ensuring the accuracy of the information being reported. Beyond that, journalists should never forget that they are also citizens with a responsibility to consider the implications of their story and to exclude their own personal biases from their content. It is irresponsible to write to inflame passions or tensions, she stressed.
As conference participants pulled away from the pier for a guided tour of New York harbor, Curator/Director of the U.S. Army's Harbor Defense Museum Justin Batt noted that not far from the tour's point of departure, former Treasury Secretary Hamilton and former Vice-President Aaron Burr began their crossing of the Hudson en route to their famous 1804 duel that killed Hamilton, but also led to Burr’s eventual political disgrace. Both men, Batt related, had served as George Washington’s personal aides during the Revolutionary War, but had become estranged afterwards, as Hamilton became de facto leader of the Federalist Party and Burr joined Thomas Jefferson’s Democratic-Republicans. Linking the story of the duel to the conference theme, Batt recalled that Hamilton’s ferocious impugning of Burr over many years in the New York press led to the fight.

Taking us further back in time, Batt recalled that New York harbor was formed 10,000 years ago when a thousand-foot deep glacier withdrew northward, leaving the openings to the Atlantic between Long Island, Staten Island, and Manhattan Island that form, historically-speaking, the most important anchorage of the United States. The first European explorers, Giovanni da Verrazzano (France – 1524) and Henry Hudson (The Netherlands – 1609) found Manhattan occupied by a sub-group of the Lenape, or Delaware, one of the larger Native American groups living along North America’s eastern seaboard. In 1626, Dutch settlers arrived and allegedly purchased Manhattan by trading beads and blankets for seashells. Batt, however, noted the seashells were considered highly valuable along the eastern seaboard, because they were an integral component for “wampum,” the tool Native Americans used to intermediate trade. Even before the arrival of Europeans, New York may have been a major financial center, commented Batt.

As the tour passed between Manhattan and Brooklyn on Long Island, Batt fast-forwarded in time to the American Revolutionary War to recount the story of George Washington’s failed effort to defend New York from British attack in 1776. After his defeat at the Battle of Brooklyn Heights, Washington and his army were trapped on Long Island between the British Army and Navy anchored in New York Harbor. However, fishermen and whalers from Marblehead, Massachusetts collected every small boat available in the vicinity, and during a foggy night, the men of Marblehead rowed the army across the narrows to Manhattan and temporary safety. Ultimately, the British drove Washington from New York and held the city until the end of the war.

During that time, the British held American prisoners of war in ships, anchored at Wallabout Bay off Brooklyn. More than 11,000 prisoners died on these vessels, nearly three times the number of Americans (approximately 4500) who died in combat, Batt noted. After the war, Wallabout Bay became a major U.S. Naval facility, now known as the Brooklyn Navy Yard. That facility built some of the most famous American warships in history, including the battleships USS Arizona, USS Iowa, and USS Missouri, aircraft carriers USS Franklin D. Roosevelt and USS Constellation, as well as the light cruiser USS Helena, recently discovered in the South Pacific by
Microsoft co-founder Paul Allen’s team. It was also the embarkation point for thousands of U.S. servicemen who sailed to Europe to fight in World Wars I and II.

Perhaps, the most interesting aspect of the tour was Batt’s recollection of the construction of New York’s iconic Brooklyn Bridge, which spans the East River and connects Brooklyn to Manhattan. The world’s first steel suspension bridge, it boasted upon its completion the world’s longest suspension span in the world, 1600 feet from tower to tower. Designed by German immigrant John Augustus Roebling, who died after an accident just three weeks after construction started, the bridge was completed by his son’s wife, Emily Roebling. Her husband, Washington A. Roebling (the designer’s son), had been partially paralyzed from “the bends,” who along with more than 100 workers (mostly immigrants working for $2/day), acquired the condition from excavating the bridge tower foundations under water. One interesting fact conveyed by Batt was that the tower on the Brooklyn side is built on bedrock, 44 feet below the East River’s bottom, but the Manhattan tower, which extends 78 feet below the bottom, never reached bedrock.

Over the course of the tour, Batt also described the fortifications that guarded New York harbor for many decades, including Castle William and Fort Jay on Governor’s Island along with Fort Hamilton where the Harbor Defense Museum is located. In addition, Batt pointed out other emblematic features of New York City, including One World Trade Center, Battery Park, and the Empire State Building. The final stop on the tour was at Ellis Island and the Statue of Liberty, at which time Mr. Batt briefed the audience on the historical importance and symbolism of both to the American narrative, closing his presentation with a reading of Emma Lazarus’ famous poem, “The New Colossus.”

“Not like the brazen giant of Greek fame,
With conquering limbs astride from land to land;
Here at our sea-washed, sunset gates shall stand
A mighty woman with a torch, whose flame
Is the imprisoned lightining, and her name
Mother of Exiles. From her beacon-hand
Glows world-wide welcome; her mild eyes command
The air-bridged harbor that twin cities frame.
‘Keep, ancient lands, your storied pomp!’ cries she
With silent lips. 'Give me your tired, your poor,
Your huddled masses yearning to breathe free,
The wretched refuse of your teeming shore.
Send these, the homeless, tempest-tost to me,
I lift my lamp beside the golden door!’”

The tour and Mr. Batt’s narrative proved strongly evocative to conference participants, prompting one to send us the following thoughts: “I personally would also like to point out the fantastic conduct of the social events - especially the boat trip around Manhattan- which held a special personal meaning to me. This was the first time since 2002 I was back to see “ground zero” - after having served at MacDill AFB as ... liaison to CENTCOM since October 2001, following the 9/11 attack. My US SOF brothers urged me to go up to New York in 2002, and actually see the center where it all started, when we were all tested by terrorists - before going home .... That visit left a lasting impression on me. It was real humbling to see the sites again here in NYC 16 years later - and this together with a host of my USSOF counterparts from that time. In retrospect I am real glad that we have been able to get so close to each other, fighting shoulder to shoulder ever since, and form this unbreakable bond and brotherhood. My country’s SOF is there whenever you need us. Thanks for your leadership, and thanks for allowing us to share the burden!”
Three of New York’s leading, young technological financiers and innovators, Jonathan Keiden of Torch Capital, Dan Keyserling from Jigsaw, and Henrik Werdelin of BAR K and Prehype, discussed a range of issues associated with the roles and responsibilities of corporations, investors, and innovators as they create new products and services that are changing societies, governments, and relationships. Keiden opened with the observation that one impact of technological change has been the blurring of lines between the public and private sectors. Companies that provide widely-used social media platforms or other innovative technologies have responsibilities that go beyond generating profits for the companies’ owners. Used negatively, these technologies can have substantial influence and impacts affecting governments, societies, and commerce both nationally and internationally. Nevertheless, Keiden said many large, public tech companies believe that their sole responsibility is to their shareholders.

Werdelin interjected that many young entrepreneurs have a wider sense of public responsibility. “I think there’s definitely a mood change ...” among entrepreneurs, he said. Many feel that we need to be more active in building technological solutions to help people who can’t feed themselves, who need adequate health care, or other major problems. But, Werdelin stressed, like the Florida teenagers after the Stoneman Douglas High School shooting, entrepreneurs have little confidence that politicians and governments have either the will or the capacity to address them.

Jigsaw, the group formerly known as Google Ideas, is, according to Dan Keyserling, motivated by the question of how technology can make the world safer. This depends on developing a shared understanding, a share vocabulary, even, of the relationship between technology companies, governments, and societies. At Jigsaw, we try to help government policy makers understand tools and technologies, how they work, how they’ll develop, as well as the effects that they’re having in the world. Likewise, we seek to explain to companies how governments view the same problem sets. There is, however, not a great deal of connective tissue between technology companies and governments, because technology companies are young, but as that connective tissue gets built, we should start creating a shared understanding of actual problems that can serve as the foundation for their solutions.

All three participants underscored their own excitement with the pace, scope, and ambition of technological innovation, while recognizing the moral dilemmas it is creating. Entrepreneurs, they said, just dive into a project, not knowing what they’re building and rarely, if ever, contemplate the unintended consequences from their inventions. Innovation is exponential, and humans often cannot cope with the rapid pace of change. For instance, the consequences on employment from artificial intelligence breakthroughs or the development of 3-D printing of rockets that could put micro-satellites into orbit could have profound implications for societies and governments. Likewise, the internet of things, powered by next generation broadband could provide tremendous growth in convenience, efficiency, and data processing, but it would still be hackable, or some 23-year old kid could shut down a power plant because he’s found a back door and is angry with his girlfriend.

Keyserling cautioned that some State and non-State actors will likely continue to exploit technology to gain advantages, so Jigsaw is working to defend news organizations from digital attacks. The press, he
continued, is often the first set of targets when State or non-State actors want to control a population. Democracies depend on an independent press to report the truth, and if we permit those institutions to be constantly threatened, we may regret it.

To establish trust among consumers, governments, and society, technology companies must take responsibility for their products and services, all three agreed. Expanding on the point, Keidan explained that transparency is the key to accepting responsibility and maintaining trust, but “[t]ransparency is more than just responsible disclosure when things go wrong.” It can be proactively achieved through open sourcing of products, engaging with peers and developers, employing trusted testers, working directly with communities, and being open to peer review. For instance, Keyserling related, there is a widely held value in the hacker community that when someone discovers a software vulnerability, it should be disclosed to the company so it can patch the problem. Ultimately, it is important for everyone to understand expectations, so we may need to work towards an unofficial understanding among people, governments, and tech companies, Keidan concluded.

All three were optimistic about the future that technology would bring, although with some startling concepts. For instance, Werdelin suggested that companies like Alibaba may very well look like a State, with its own cryptocoin, security teams, and other State-like attributes. And Estonia, a country, may allow people from anywhere in the world to apply for digital citizenship, social security number included, without actually having a passport there. Keidan tempered that view somewhat, noting that the Chinese government would certainly continue to have a say in the operating behavior of companies like Alibaba, Tencent, and WeChat. Nevertheless, at the end of the day, as Werdelin said, if you are a positive person, then you believe that people are trying to be safe and secure and feed their families, and those values will tend to prevail over greed.
During the final plenary, break out group spokespersons shared highlights of their discussions about the major themes presented during the previous three days. Media responsibility and accountability, education to improve the general populace’s listening and critical thinking skills, the moral neutrality of technology, the need for systems of shared responsibility for technology users, and the critical importance of local history, customs, and values for shaping effective narratives emerged as concepts that resonated with participants.

One participant observed that the world’s public will always crave news and information, but the problem in a competitive media environment is evaluating available information. A second participant acknowledged the importance of access to a wide variety of media outlets, but also stressed that assessing truth becomes progressively more difficult in such an environment. To address this problem set effectively, the first commentator recommended active cooperation among consumers, media organizations, and governments to improve media responsibility for the material they present and to hold media accountable for whatever they communicate. Better media self-regulation, such as we see with many on-line game sites or Wikipedia, may be the best option, he concluded, but better government oversight is also required. However, as one final presenter said, “… our goal should be an information sector that lives up to our values, rather than operates down to laws and regulations.”

A well-educated and well-informed public will be able to discern false narratives more easily, suggested one participant. Thus, educating our respective publics, especially in critical thinking skills, will better enable them to meet the challenges of false narratives and hold their disseminators accountable, added two other group spokespersons.

Two spokespersons underscored that we should see technology as only a tool that can be used either positively or negatively. Even when technology helps solve a problem, it can create unintended consequences, as we are seeing with Facebook. Our challenge, a third participant added, is the thoughtful and timely integration of technology to measure, evaluate, and communicate. We saw at the New York Police Department that the thoughtful application of technology can achieve significant outcomes for the public. As we heard in the presentation, the NYPD believes its integration of technology into its operations came late, but we may be even later to that task than the New York Police Department.

It is clear, another spokesman stressed, that totalitarian and rogue states that are not bound by rule of law and the democratic way of life are exploiting technology to conduct disinformation operations
to gain strategic advantage. Likewise, a second participant added, ISIS and other terrorist groups are mounting technologically sophisticated, well-coordinated information campaigns.

Another participant underscored that “we need to craft effective narratives that will resonate with local populations, like some of the hostile groups that we have been engaging.” We need to do a better job of learning local history and customs to identify appropriate messengers, messages, and mediums for winning narratives, he emphasized. Along the same lines, a participant added that a local approach using soft sources like social and digital media, which is culturally acceptable for the people, could be the best approach to counter radicalized extremist ideologies. A third participant recommended that social groups, NGOs, and other such organizations could be instrumental in crafting effective alternative messaging.

Listening, a commenter suggested, might be the first step in building effective narratives. Africa, and Africans, he said, are simply asking to be listened to, so that non-Africans may identify relevant themes, rather than imposing solutions. This, he continued, will not be easy, because Africa comprises 54 countries, and each has its own cultural norms, attitudes, and values which should be respected. Leveraging platforms like Sovereign Challenge allows people to gain deeper understanding of different perspectives.

Today, Africa is a set of young countries, young democracies, looking for development to bring its peoples out of poverty, to reduce disease, and to increase education. Africa is a continent endowed with remarkable resources, both human and material, but Africa needs assistance managing them. Today, we would like to see you invest in a joint future with us. We would welcome improved education so that we may adapt to these new technologies for the betterment of our people.

“The question was asked, ten years from now, what do you see your society as looking like? And the answer is we don’t know because the world is so dynamic. There are so many changes taking place and so rapidly. The majority of us like to tease ourselves and say that we are BBC, born before computers. In my country the guys are so fast. You can give your son something to play with that in no time he’s sorted it out. We are grappling with it. So, what you want to do is invest in us, allow us to understand all these various mediums so that we can use it for the betterment of our societies.”
Speaker Biographies

Mr. William J. Miller, **Director of Strategy, Plans, and Policy**, U.S. Special Operations Command. Upon graduation from the University of Florida, he received commission as a 2nd Lieutenant in the cavalry. In his 26-year Army career, he led and commanded U.S. and allied Soldiers from the platoon through brigade level. He has extensive operational experience, including numerous deployments to Kosovo, Bosnia, Kuwait, Iraq, and Afghanistan.

Mr. Zahed Amanullah, **Head of Networks and Outreach**, Institute for Strategic Dialogue. Zahed Amanullah has co-authored numerous reports on the Islamic State and how it has successfully promoted its narrative. He has also recently co-authored a report on online information campaigns during the 2017 Kenyan elections. As such, he can discuss narratives information campaigns in both Africa and the Middle East.

Mr. Justin M. Batt, **Curator/Director of the Harbor Defense Museum**, at USAG Fort Hamilton. Mr. Batt is a curator with the Army Museum Enterprise. The Army Museum Enterprise (AME) serves as the repository and steward for the U.S. Army’s material culture. The mission of the AME is to train, honor and inspire soldiers, and public education regarding the history of the U.S. Army. Mr. Batt has over 10 years’ experience with the AME, working at the U.S. Army War College, National Infantry Museum, National Armor and Cavalry Museum and the Harbor Defense Museum. Prior to working for the AME Mr. Batt was a seasonal park ranger at Rocky Mountain National Park.

Mr. Charles E. Berger, **Assistant Special Agent-in-Charge**, Federal Bureau of Investigation New York Field Office. A 19-year FBI veteran, Mr. Berger specializes in counterterrorism and national security. Prior to the FBI, Mr Berger served as a U.S. Navy flight officer for 12 years. Mr. Berger has written extensively on national security, most recently co-writing Guaranteeing America’s Security in the Twenty-First Century, a guide to national security for practitioners.

Ms. Elisabeth Braw, **Nonresident Senior Fellow, Scowcroft Center for Strategy and Security**, Atlantic Council. Previously a correspondent for the *Christian Science Monitor* and *Newsweek*, she is a regular contributor to *Foreign Affairs* and *Foreign Policy*, specializing in European security. In addition, she writes the *Transatlantic Connection* blog for the *World Affairs Journal*. Elisabeth is a native of Sweden and attended university in Germany, finishing her Magister Artium degree in political science and German literature with a dissertation on nuclear weapons reduction in Europe.

Mr. Steve Clayton, **Chief Storyteller**, Microsoft. Steve Clayton is Microsoft’s Chief Storyteller and General Manager of Microsoft’s Image, Culture and AI Communications team. The team is responsible for shaping the company’s image, telling its culture story and sharing its AI strategy – internally and externally – through storytelling. Steve was the architect of the acclaimed “88 Acres” story that heralded a new direction for Microsoft’s corporate storytelling and led to the creation of microsoft.com/stories. His team creates a wide variety of content including keynote demos for Satya Nadella, Microsoft’s AI blog, Microsoft Life as well as operating the company intranet.

Mr. Yarema Dukh, **Special Assistant to the Press Secretary of the President of Ukraine**, Presidential Administration of Ukraine. As profiled by the Wall Street Journal, Dukh has led social media campaigns for Ukraine’s government to promote Ukraine and counter Russian disinformation and cyber activity. He provides a unique government perspective to the second panel.
Mr. Maxim Eristavi, Research Fellow, Eurasia Center, Atlantic Council
A prominent Eastern European media activist, Maxim Eristavi has helped start various media movements in Eastern Europe. In 2014, he co-founded Hromadske International, an independent news outlet that covers central and Eastern Europe.

Mr. James P. Farwell, CEO, Farwell Group
Author, national security expert, attorney, and Certified Information Privacy Professional (CIPP/US), expert in cyber policy and strategic communication. Author of Persuasion and Power: The Art of Strategic Communication, The Pakistan Cauldron: Conspiracy, Assassination, & Instability, and a new opera, “The Fabulist,” that is being produced by Tony-Award winning producer Steven Levy. Associate Fellow, Centre for Strategic Communication, Department of War Studies, Kings College, U. of London and non-resident Senior Fellow, Middle East Institute in Washington, D.C.

Mr. Wil van Gemert, Deputy Executive Director of Europol, Operations Directorate, Europol
On 1 May 2014, Mr van Gemert took up the position of Deputy Director of Europol and Head of the Operations Department. He manages a department of experts, specialists and analysts dealing with serious and organised crime, as well as terrorism and cybercrime. Previously, Mr. van Gemert served the Royal Netherlands government as Director of Cyber Security and Director of National Security for the Dutch National Intelligence Service.

Mr. Marcel Granier, Former President, Radio Caracas Television
As the former CEO of Radio Caracas Television (RCTV), Granier was faced with a significant challenge when the Venezuelan government attempted to shut down the network in 2002. This experience is one of many that makes him qualified for addressing how governments work to control media narratives from a Latin American perspective.

Dr. Richard Haass, President, Council on Foreign Relations
Dr. Richard Haass is in his fifteenth year as president of the Council on Foreign Relations, an independent, nonpartisan membership organization, think tank, publisher, and educational institution dedicated to being a resource to help people better understand the world and the foreign policy choices facing the United States and other countries. In 2013, he served as the chair of the multiparty negotiations in Northern Ireland that provided the foundation for the 2014 Stormont House Agreement. Dr. Haass has extensive U.S. government experience including service from 2001-2003 as Director of Policy Planning for the U.S. Department of State.

Mr. Jakub Kalensky, Member, East StratCom Task Force, European External Action Service
The East Stratcom Task Force is the European Union’s organization for countering disinformation. Jakub has been tracking disinformation from state and non-state actors across all 27 EU member states. Through sites through EUvsDisinfo, the Task Force works to combat disinformation narratives, and Jakub can provide an overview of the EU’s strategy and efforts.

Mr. Jonathan Keidan, Founder, Torch Capital, Co-Founder, InsideHook
Jonathan has spent his career at the intersection of the media, technology, and entertainment industries. He is the Co-Founder of digital media company, InsideHook, and the Founder of Torch Capital, an early stage venture fund that has backed a number of New York & LA’s top consumer start-ups (e.g., Compass, Zoc Doc, Acorns (also an advisor), Sweetgreen, Laurel & Wolf, Sir Kensington’s, Bounce Exchange, Virtru, Nadaam, among others).
**Speaker Biographies**

**Mr. Dan Keyserling, Head of Communications, Public Affairs, and Operations, Jigsaw**
Dan oversees Jigsaw’s communications and public affairs. Prior to joining Google in 2010, Dan worked for The New York Times and at the University of Virginia Center for Politics, a nonpartisan think tank devoted to studying American politics and civic engagement. Dan started his career in the “War Room” of Hillary Clinton’s 2008 presidential campaign assisting with rapid response efforts.

**Dr. Ajit Maan, President, Narrative Strategies**
As the president of Narrative Strategies, Maan works with former special operations professionals to discuss the impact that disinformation and “fake news” can have. Her research has focused on influence in unconventional warfare, as well as how self-identity can impact the influence that political information campaigns can have.

**Ms. Maria Ressa, Chief Executive Officer, Rappler**
Maria Ressa is the founder and CEO of Rappler, an independent Filipino news outlet. Rappler has faced various attempts to limit its journalistic freedom, and Ressa provides an expert voice on government attempts to control the media narrative in Asia.

**Ms. Susan Sim, Vice President for Asia, The Soufan Group**
Following a career in government (including as an intelligence analyst and diplomat), as well as in journalism, Susan Sim joined a panel of leading national security experts gathered by The Soufan Group to study terrorist risk reduction programmes and countering of extremist narratives. Having served in both Singapore and Indonesia, she provides a Southeast Asian perspective to the conference.

**Mr. Andrei Soldatov, Co-Founder and Editor, Agentura.ru**
Co-author of The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries and The New Nobility: The Restoration of Russia’s Security State and the Enduring Legacy of the KGB with Irina Borogan, Andrei Soldatov co-founded with Borogan the Agentura.ru project to monitor Russian state surveillance activities. A graduate of Russian State Social University in journalism, Soldatov has extensive journalist experience covering both Russian domestic and international topics.

**Mr. Henrik Werdelin, Co-founder, BARK; Founding Partner, Prehype**
Henrik Werdelin is the co-founder of BARK (BarkBox) as well as Founding Partner of Prehype, a venture development firm headquartered in New York with offices in London and Copenhagen. Henrik has been part of the startup scene since 2005 as both an investor, founder and advisor. His experience ranges from being Entrepreneur in Residence at Index Ventures to working with, advising or investing in start-ups like HotPotato (now Facebook), GoTryItOn (now Rent the Runway), ReadMill (now DropBox) and Sunrise (now Microsoft). Before being an entrepreneur/angel, Werdelin was Vice President of Product Development and Strategy for MTV Networks International spearheading the development of many of MTV’s award winning products.

**Ms. Patience Zirima, Director, Media Monitors Zimbabwe**
Patience Zirima directs Media Monitors Zimbabwe, an organization that works to promote freedom of expression and responsible journalism in Zimbabwe through monitoring news media. This makes her ideal for speaking on combatting disinformation from an African perspective.
Acknowledgements

Atlantic Council

HQ U.S. Special Operations Command and its Sovereign Challenge program gratefully acknowledge the contributions of the Council on Foreign Relations, The Atlantic Council, and the New York Police Department to this conference. Their partnership in this event was essential to its success.