United States Department of State

Washington, D.C. 20520

March 29, 2024

Case No. FL-2023-00013

Reed Rubinstein
America First Legal Foundation
611 Pennsylvania Avenue, SE, #231
Washington, DC 20003

Dear Mr. Rubinstein:

As we noted in our letter dated February 29, 2024, we are processing your request for material under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. The Department of State ("Department") has identified seven additional responsive records subject to the FOIA. Upon review, we have determined that all seven records may be released in part.

An enclosure explains the FOIA exemptions and other grounds for withholding material. Where we have made redactions, the applicable FOIA exemptions are marked on each record. Where applicable, the Department has considered the foreseeable harm standard when reviewing these records and applying FOIA exemptions. All non-exempt material that is reasonably segregable from the exempt material has been released and is enclosed.

We will keep you informed as your case progresses. If you have any questions, your attorney may contact Kevin Bell, U.S. Department of Justice Trial Attorney, at kevin.k.bell@usdoj.gov and (202) 305-8613. Please refer to the case number, FL-2023-00013, and the civil action number, 22-cv-03386, in all correspondence about this case.

Sincerely,

Diamonece Hickson
Chief, Litigation and Appeals Branch
Office of Information Programs and Services

Enclosures: As stated.

The Freedom of Information Act (5 USC 552)

FOIA Exemptions

(b)(1) Information specifically authorized by an executive order to be kept secret in the interest of national defense or foreign policy. Executive Order 13526 includes the following classification categories:

1.4(a) Military plans, systems, or operations
1.4(b) Foreign government information
1.4(c) Intelligence activities, sources or methods, or cryptology
1.4(d) Foreign relations or foreign activities of the US, including confidential sources
1.4(e) Scientific, technological, or economic matters relating to national security, including defense against transnational terrorism
1.4(f) U.S. Government programs for safeguarding nuclear materials or facilities
1.4(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to US national security, including defense against transnational terrorism
1.4(h) Weapons of mass destruction

(b)(2) Related solely to the internal personnel rules and practices of an agency

(b)(3) Specifically exempted from disclosure by statute (other than 5 USC 552), for example:

ARMSEXP	Arms Export Control Act, 50a USC 2411(c)
CIA PERS/ORG	Central Intelligence Agency Act of 1949, 50 USC 403(g)
EXPORT CONTROL	Export Administration Act of 1979, 50 USC App. Sec. 2411(c)
FS ACT	Foreign Service Act of 1980, 22 USC 4004
INA	Immigration and Nationality Act, 8 USC 1202(f), Sec. 222(f)
IRAN	Iran Claims Settlement Act, Public Law 99-99, Sec. 505

(b)(4) Trade secrets and confidential commercial or financial information

(b)(5) Interagency or intra-agency communications forming part of the deliberative process, attorney-client privilege, or attorney work product

(b)(6) Personal privacy information

(b)(7) Law enforcement information whose disclosure would:
(A) interfere with enforcement proceedings
(B) deprive a person of a fair trial
(C) constitute an unwarranted invasion of personal privacy
(D) disclose confidential sources
(E) disclose investigation techniques
(F) endanger life or physical safety of an individual

(b)(8) Prepared by or for a government agency regulating or supervising financial institutions

(b)(9) Geological and geophysical information and data, including maps, concerning wells

Other Grounds for Withholding

NR Material not responsive to a FOIA request excised with the agreement of the requester

From: "Ice, John T" (b)(6) @state.gov>
To: Lee, Matthew (b)(6) ap.org>
CC: (b)(6) state.gov>;
(b)(6) state.gov>
Subject: Re: Response to Taken Questions
Date: Wed, 4 Nov 2020 22:23:10 +0000

No worries, Matt. Talk to you, then.
J.T.
From: Lee, Matthew (b)(6) ap.org>
Sent: Wednesday, November 4, 2020 5:18 PM
To: Ice, John T (b)(6) state.gov>
Cc (b)(6) state.gov> (b)(6) @state.gov>
Subject: Re: Response to Taken Questions

Hey there:
I'm sorry. We're so swamped with election stuff I haven't gotten an answer. Can I get back to you tomorrow morning?
Thanks,
Matt

On Nov 4, 2020, at 5:14 PM, Ice, John T (b)(6) @state.gov> wrote:

[EXTERNAL]
Hi Matt,
Off the record, realizing there is a lot going on, we wanted to touch base on this. Are you still looking to put something together? If not, let us know and we will begin to look at other options.
Best,
J.T.
From: Ice, John T (b)(6) @state.gov>
Sent: Monday, November 2, 2020 11:34 AM
To: Lee, Matthew (b)(6) ap.org>
Cc (b)(6) state.gov>; (b)(6) @state.gov>
Subject: Re: Response to Taken Questions

Hi Matt,
I hope that you are at least somewhat recovered from the trip. Bumping this up to the top of your email queue.
Best,
J.T.
From: Ice, John T (b)(6) state.gov>
Sent: Thursday, October 29, 2020 3:35 PM

To: Lee, Matthew (b)(6) ap.org>
Cc: (b)(6) state.gov>
Subject: Response to Taken Questions

Hi Matt,
Following up on the conversation last week, below are GEC's responses to the two taken questions.
These responses are provided on deep background.

Q1. How are people getting to these sites? Google? Etc

The majority of users accessing these four sites go to the site directly. For greater context, we have outlined the traffic for each of the four sites below. This data captures traffic for the full month of September from SimilarWeb, a publicly available tool.

Definitions:
Direct traffic occurs when a visitor arrives directly on a website by typing in the website's URL, without having clicked on a link on another site or using a search engine.
Referral traffic describes the people who come to a domain from other sites, without using a search engine.
Search traffic refers to the visitors who arrive at a website by clicking search results leading to that particular website (mostly after searching keywords or phrases).
Social traffic is traffic from social media outlets.

- **NEO**: 79% direct traffic; 8.5% referral traffic (mostly from other alternative media); 7.7% traffic from search; 3.7% social traffic (43.6% from Facebook)
- **Oriental Review:** 55.5% direct traffic; 13.3% referral traffic (83% from news aggregator Inoreader); 21.4% from search traffic; 9.7% social traffic (56% from Twitter)
- **News Front:** 63.9% direct traffic; 13.5% referral traffic (33% from Russian search engine Yandex; other traffic from news aggregators and websites); 5.9% from search traffic; 9.8% social traffic (56.8% VKontakte)
- **Rebel Inside:** Not available on SimilarWeb.

Q2. Are we seeing lots of Spanish speaking audiences targeted from these sites?

News Front is the only one of the four entities we outlined that directly targets Spanish speaking audiences. News Front has a dedicated Spanish-language proxy site and claims that the site's editorial branch is based in Spain. In addition, we see that News Front targets Spanish speaking audiences on the Russian social media platform VKontakte. The page self identifies as being located in Madrid, Spain and has 1,633 followers. News Front's Spanish-language no longer has any pages on Twitter, Facebook and YouTube because they all have been suspended by the platforms.

Happy to discuss any proposal to move something to "on background."
Finally, could you give some idea about when you are looking to publish?
Best,
J.T.

John T. Ice
Deputy Spokesperson
United States Department of State
(b)(6)
(b)(6) @state.gov

Sender: "Ice, John T" (b)(6) @state.gov>
Lee, Matthew (b)(6) @ap.org>;
Recipient: (b)(6) @state.gov>;
(b)(6) @state.gov>

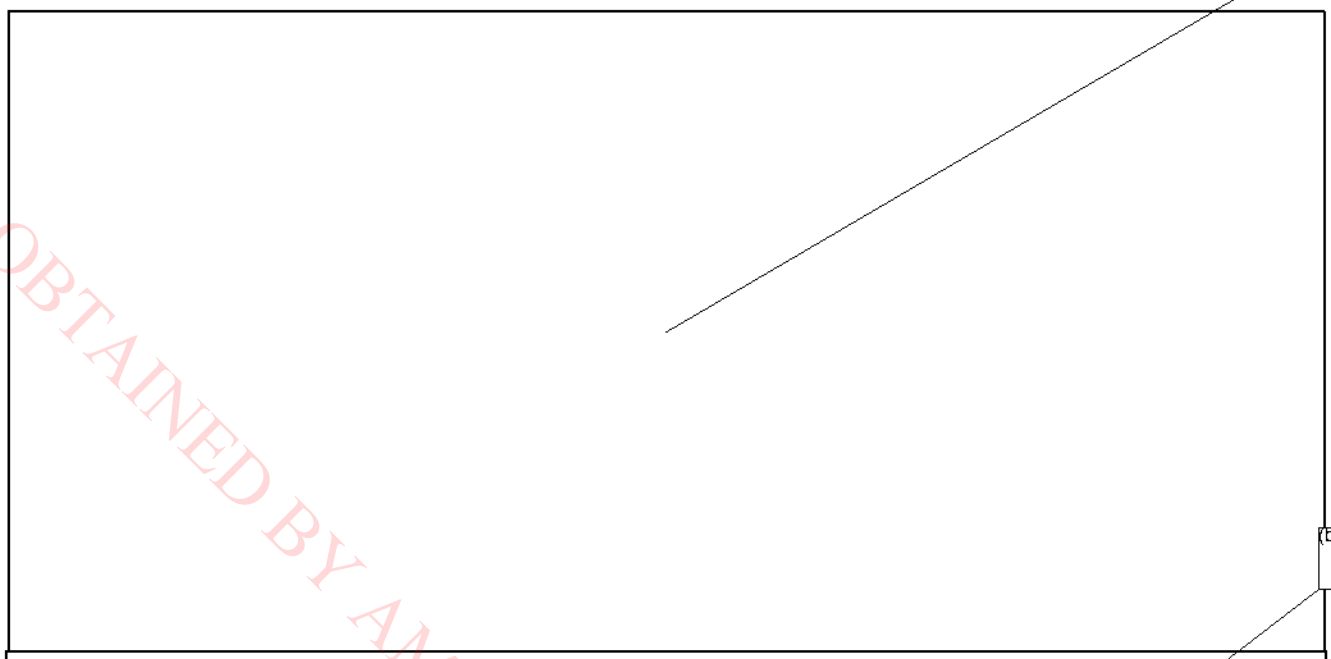
From: (b)(6) state.gov>
To: (b)(6) state.gov>; (b)(6) state.gov>; (b)(6) state.gov>
Subject: Re: First Compound Report on Russian Proxy Outlet Narratives Surrounding the 2020 U.S. Presidential Election
Date: Fri, 30 Oct 2020 12:34:42 +0000

(b)(6) -- have you reviewed (b)(6) write-up, and is it good to go to the broader election distro list?
(b)(6) -thanks for sharing with (b)(6).
Great work, (b)(6)
Best, (b)(6)
Sent from my BlackBerry 10 smartphone.
From (b)(6)
Sent: Thursday, October 29, 2020 9:14 PM
To: (b)(6)
Subject: First Compound Report on Russian Proxy Outlet Narratives Surrounding the 2020 U.S. Presidential Election

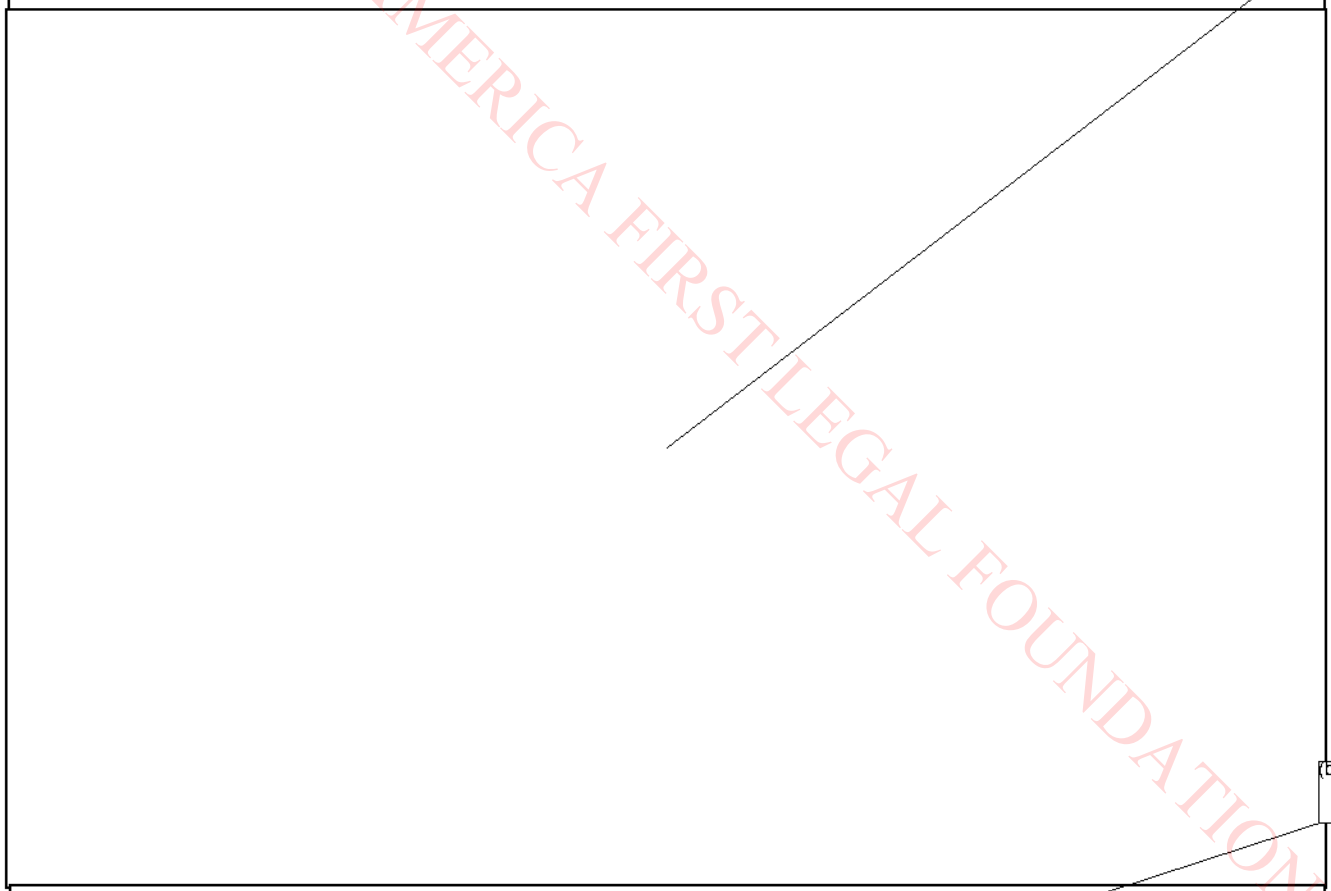
All,
(b)(6)
Please find below a compound writeup of FireEye's and my own reporting on known actors in Russia's disinformation and propaganda ecosystem promoting narratives on Hunter Biden in the lead up to the U.S. presidential election. Our FireEye contact confirmed approval for us to pull from their report however we saw fit and deferred to us on whether or not to credit them in the email we send out. When sends the email to FBI (and others?), I recommend we add a line that explains that there will be an email on the other system with some additional attribution information. In terms of wider USG distribution, I defer to you three on which partners this should go to.
One ask: Please read through the email carefully for any errors, as fusing two works together can make it difficult to catch mistakes or conflicting data points. Additionally, please scan through the original FireEye report to ensure I didn't exclude something you think should be included in the below writeup. Feel free to call with any questions or comments. -W

(b)(5)

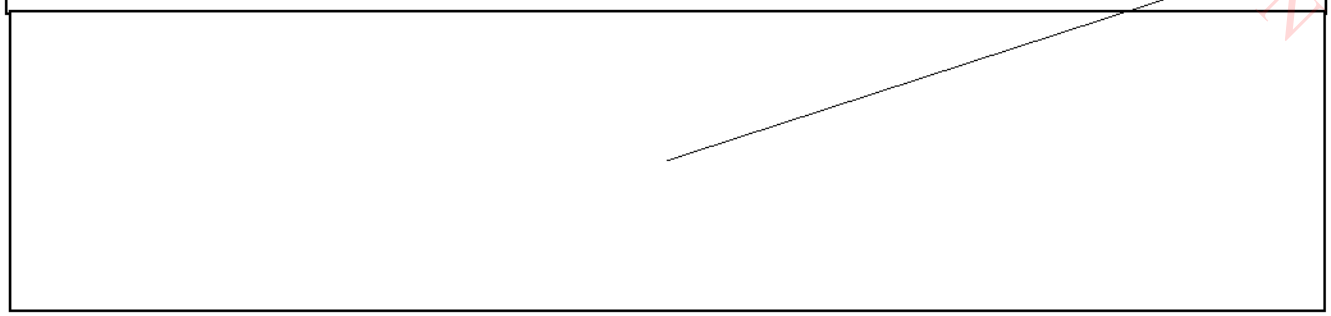
(b)(5)



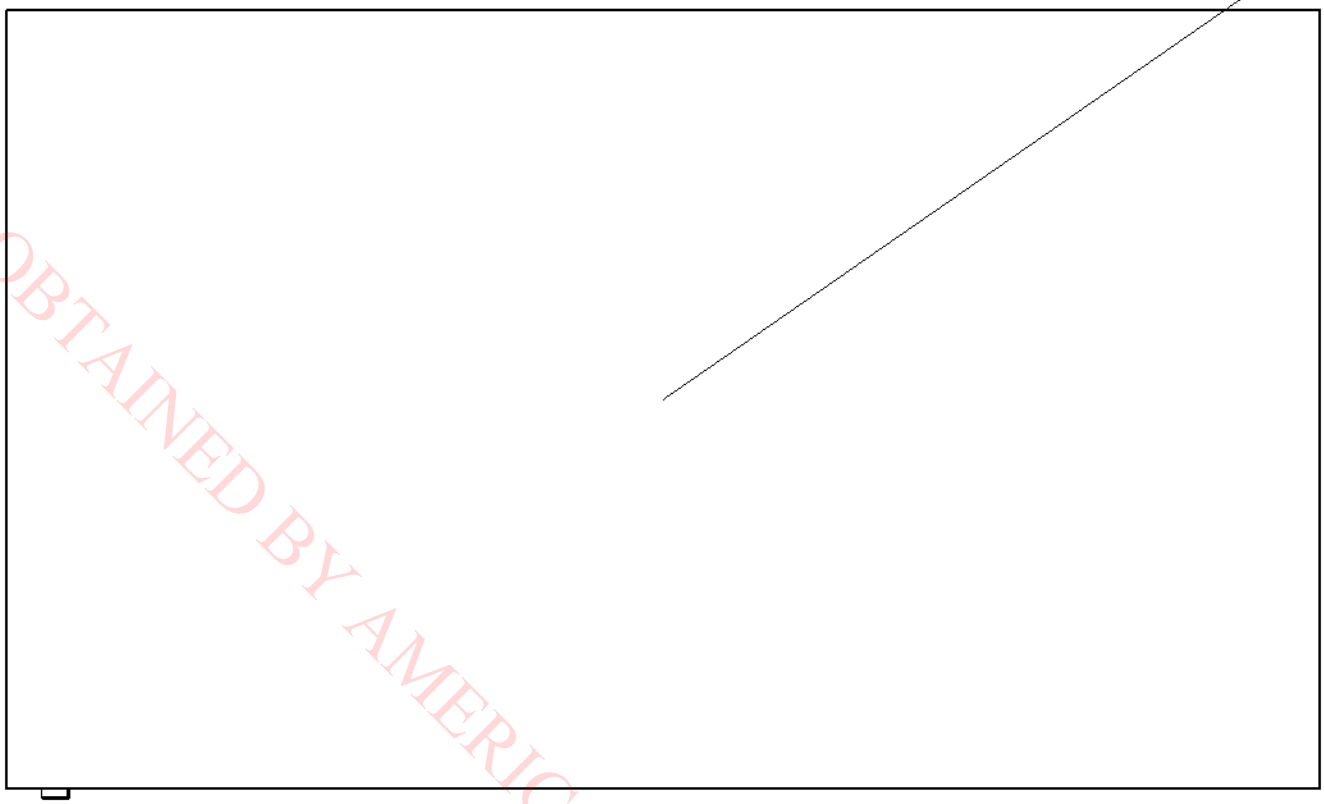
(b)(5)



(b)(5)

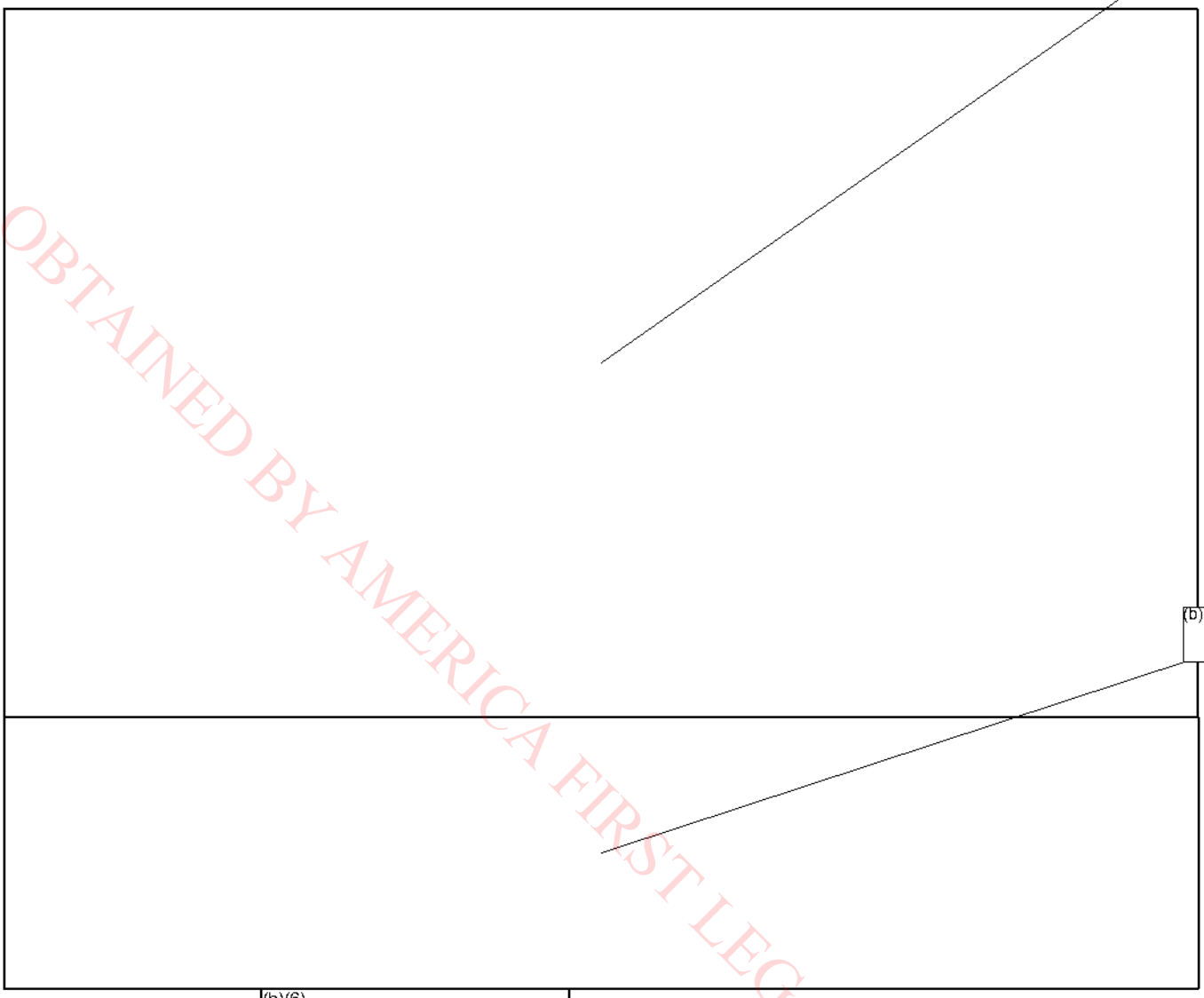


(b)(5)



(b)(5)

(b)(5)



(b)(5)

Sender: (b)(6) @state.gov>

Recipient: (b)(6) @state.gov>;
(b)(6) @state.gov>;
(b)(6) @state.gov>

From: (b)(6) state.gov>
To: (b)(6) america.gov>
Subject: Fw: Russia Highlights for December
Date: Wed, 16 Dec 2020 15:57:13 +0000

From: (b)(6) @gmail.com>
Sent: Wednesday, December 9, 2020 7:30 PM
To: (b)(6) @state.gov>
Cc: (b)(6) @gmail.com>; (b)(6) @gmail.com>
Subject: Russia Highlights for December

Good evening (b)(6)

You'll find below and attached the Russia Highlights for December. Please let us know if there is anything further needed. Happy holidays!

Best,
(b)(6)

UNCLASSIFIED

ACADEMIC & THINK TANK HIGHLIGHTS
GLOBAL ENGAGEMENT CENTER
December 2020

Dear Readers,
We track close to 100 academic and think-tank sources to bring you GEC's Academic & Think-Tank Highlights.
Please click here to take our brief survey to help improve this product and its circulation.
Thank you,
(b)(6)

Please note these summaries of academic research are compiled with the help of students and are for informational purposes only; they do not imply USG endorsement of the views expressed in the articles or their summaries. To receive GEC Academic & Think-Tank Highlights on Countering China's, Iran's, Russia's, and/or Terrorist/Violent Extremist's Propaganda and Disinformation please email (b)(6) @state.gov or visit GEC IQ.

(b)(6)

Countering Russian Disinformation
Academic & Think-Tank Highlights
December 2020

EXECUTIVE SUMMARY: RT uses Soviet-era organizational behavior to produce anti-Western content, pro-Kremlin outlets launder disinformation by intentionally mistranslating foreign media outlets, and the Wagner Group spearheads information operations in Africa. Meanwhile, research indicates that inauthentic Twitter accounts can be identified by an algorithm that assesses only behavioral features. Source labeling and media literacy interventions reduce engagement with Kremlin disinformation. Prior engagement and agreement with fake news may better predict the likelihood of sharing disinformation, and conspiracy theorizing fulfills psychological needs. Additionally, analysis of the U.S. presidential election shows links between domestic and international disinformation framing, reinforces the need for a whole-of-society approach to election integrity, and considers the impact of Covid-19 and Covid-19 misinformation on election administration. Finally, in the policy realm, gaps left by media platforms might be filled by EU regulation and the US could use increased messaging to Russian citizens to achieve a variety of goals.

ACADEMIC/PEER REVIEWED:

The RT news network uses Soviet-era organizational behavior to produce anti-Western content in accordance with the goals of Russian state defense policy: Professional journalistic skills are not prioritized in the hiring process. Following hiring, a socialization process fosters loyalty and conformance to RT's organizational practices. Such practices most prominently include self-censorship and media distortion. Through these methods, RT is able to fulfil three goals: first, to push the idea that Western countries have as many problems as Russia; second, to encourage conspiracy theories about media institutions in the West in order to discredit and delegitimize them; and third, to create controversy about RT, making it appear that the channel is important. (Mona Elswah and Philip N. Howard, Oxford Academic Journal of Communication, "Anything that Causes Chaos": The Organizational Behavior of Russia Today (RT), October 2020)

Inauthentic Twitter accounts can be identified by an algorithm that assesses only behavioral features: An algorithm using behavioral rather than linguistic features eliminates the need for language-specific processing and therefore provides more utility. The relevant behavioral features included above-average number of retweets, hashtags, URLs, and replies. Additionally, because inauthentic accounts are operated by state agency employees, activity is higher during weekdays and regular office hours. Identifying inauthentic accounts based solely on behavior can be enriched by considering other behavioral features of employee-run inauthentic accounts and by evaluating behavior-based algorithms against more diverse sets of accounts. (Saleh Alhazbi, IEEE Access, Behavior-Based Machine Learning Approaches to Identify State-Sponsored Trolls on Twitter, November 2020)

Prior familiarity with fake news stories as well as the belief that these stories were likely to be true and aligned with users' pre-existing values consistently predicted the likelihood that

users would share disinformation, whereas the measure of digital literacy, authoritativeness of a source, and a posts popularity did not: In contrast to past research on personality and social media behavior, lower levels of agreeableness and higher levels of extraversion are associated with a greater probability of sharing or liking stories. This study implies that interventions are likely to be most effective when targeted at individuals who already hold an opinion or belief, rather than interventions attempting to change people's minds. In addition, repeated exposure of disinformation materials increases the likelihood of sharing them even if users do not believe them. (Tom Buchanan, PLOS ONE, Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation, October 2020)

THINK-TANK ANALYSIS:

Increased messaging to Russian citizens is more symmetrical than a cyber operation, is less likely to spillover to other domains, and can be targeted to achieve a variety of goals: Increasing efforts to communicate directly with Russian citizens "might even add stability to the US-Russian relationship by establishing a balance of information power." Direct forms of communication could be used for several purposes: in case communication needs are urgent, to encourage incremental change, to inflame discontent, as a public diplomacy medium, or to demonstrate American capacity to penetrate Russia's information environment. The US could address Russians directly or work with non-governmental activists. But any strategy "must include alternative technical options" to remain effective in the face of Russian internet shutdowns or censorship efforts. (Thomas Kent, The Jamestown Foundation, US Messaging to Russian Citizens: Time to Step It Up?, November 2020)

Pro-Kremlin outlets launder disinformation by intentionally mistranslating foreign media outlets: Outlets peddling disinformation first identify an article in a respected foreign media outlet on a topic which is related to the narrative that the pro-Kremlin outlet wants to advance. Next, an original Russian-language piece is written that misquotes or misrepresents quotes from the reputable foreign media article, even going so far as to falsify information. The Russian language article is then translated into another language and published in an outlet that appears unrelated to pro-Kremlin outlets. This form of disinformation laundering is difficult to spot because it requires competency in several languages. (EUvsDisinfo, From English into Russian into Czech: Re-Translation as a Manipulative Tool, October 2020)

"Dispatched in dozens of countries, the Wagner Group has been tasked with implementing the Kremlin's foreign policy and deploying aggressive tactics, such as industrial-scale manufacturing of fake news, intimidation of journalists and political opponents, election interference" and more: Russian interests in Africa include lucrative security and mining contracts as well as creating a sphere of influence to direct General Assembly of the United Nations votes in Russia's favor. In addition to conventional soft power initiatives, Russian financial support for the Central African Republic's cash-strapped media sector contributes to its use as a pro-Russia propaganda tool. Counter disinformation efforts will require financial support to substitute for Russian money as well as an acknowledgment of and engagement with high rates

of illiteracy. (Nathalia Dukhan, Atlantic Council, Central African Republic: Ground Zero for Russian Influence in Central Africa, October 2020)

Voting-specific narratives of the last presidential election link isolated issues in an attempt to prove that there was a vast conspiracy determining the outcome, and that therefore the outcome is fraudulent: If believed by a large number of Americans, these delegitimization narratives constitute a major concern, however any intervention against domestic disinformation risks being cast as censorship. New platforms like Parler promote their services on the basis of freedom of speech, but because Parler lacks an election integrity team—like those employed by Facebook and Twitter to flag misinformation—their service is easily targeted for monetary and ideological purposes. Disinformation campaigns run continuously both domestically and internationally, but by monitoring social media, false narratives can be identified early enough for fact checkers to limit their impact. (Freeman Spogli Institute for International Studies, Society Needs to Adapt to a World of Widespread Disinformation, October 2020)

In the short term, the U.S. has been slow to adapt to emerging threats from authoritarian states, but can regain advantage in the long term via four spheres of competition: political, economic, technological, and informational: Authoritarians exploit democracies' openness, manipulate information, and penetrate permissive political influence systems, but the U.S. can respond by strengthening key institutions, cultivating civic engagement, and highlighting the corruption and political repression of autocracies. The U.S. must make strategic investments at home—including in infrastructure, education, and basic research—while also supporting innovation and development in key industries. The U.S. should work with other democracies to shape global technology governance to ensure that norms, standards, and new technologies are conducive rather than corrosive to democracy. Trusted information is the foundation of a healthy society, and democracies need to counter threats of authoritarian interference in the information space without compromising the democratic value of free expression. To do so, the United States should embrace media and digital literacy education, ensure that information architecture supports democratic values, challenge authoritarian narrative dominance, and reinvigorate independent journalism. (Alliance for Securing Democracy, Linking Values and Strategy: How Democracies Can Offset Autocratic Advances, October 2020)

THREAT AGNOSTIC:

Source labeling and media literacy interventions reduce engagement with Kremlin disinformation: IREX's Learn to Discern approach revealed several key findings on the effect media literacy messaging could have on social media users. Kremlin propaganda evokes emotional responses, which drives propaganda's rapid spread. However, brief media literacy interventions of only two minutes can shift behaviors of hard-to-reach groups with the strongest effect on partisan news consumers. Labeling propaganda with its source also reduces the likelihood that partisan participants will like/share content, and the two interventions are complementary. The trial results are promising, but further research is required to understand more about specific types of media literacy messages, the audiences they best influence, and the effects of different levels of exposure. (IREX, Randomized Control Trial Finds IREX's Media Literacy Messages to be Effective in Reducing Engagement with Disinformation, October 2020)

The majority of misinformation narratives about the 2020 election originated from domestic actors and have been utilized by foreign state actors and media to sow domestic and foreign distrust in the U.S. political system: After the 2020 presidential election, there has been a strong influx of false and misleading information about the validity of the election results and the integrity of the voting process. The election received large amounts of coverage from Russian and Iranian state media, while Chinese state media accounts provided far less. Russian and Iranian state media served as amplifiers of false and misleading information, often retweeting prominent American outlets or individuals, with a heavy reliance on President Trump's twitter feed to advance claims mentioning "fraud, "rigged" or "steal." China, however, added disclaimers to its retweets, indicating that claims were "unproven" or "unsubstantiated." Each country's amplification of misinformation narratives (or lack thereof) reflects their preferences in information strategies as well as their preferences between the two presidential candidates. Additionally, all three countries have provided significant coverage of unrest and sporadic violence in the U.S., following a pattern of exaggerating the supposed decline of U.S. society. (Bret Schafer, Alliance for Securing Democracy, Foreign Amplification of Voter Fraud Narratives: How Russian, Iranian, and Chinese Messengers Have Leveraged Post-Election Unrest in the United States, November 2020)

A recent study from the UK found that because of current widespread misinformation, there remains high uncertainty regarding public vaccination intentions, and for community protection to be achieved, at least 80% of the community must be vaccinated: In order to overcome this hesitancy and ensure effective coverage is achieved, governments must start an open dialogue with the public regarding vaccine deployment, which is critical to build support about who has vaccination priority, address fears about safety, communicate complex information about multiple vaccines, and counter misinformation and public complacency. The most pressing challenges include making vaccinations convenient by building on existing immunization programs, implementing decentralized local vaccination programs tailored to community needs, adopting transparent principles of vaccination priority groups including sufficient public debate, empowering the public to spot and report misinformation, and ensuring accountability for media companies to remove harmful information and punishing those who spread misinformation. (Melinda Mills, The British Academy,Vaccine Hesitancy Threatens to Undermine Pandemic Response, November 2020)

Technological leadership by the world's major liberal-democratic nations will be essential to safeguarding democratic institutions, norms, and values, and will contribute to global peace and prosperity: Those who shape the use of emerging technologies will garner economic, military, and political strength for decades. A unified approach by like-minded nations is needed to counteract growing investments in and deployments of emerging technologies by authoritarian, revisionist powers. To that end, a technology alliance should be formed; the writers offer a blueprint to move from concept to actionable items, offering a summary of 13 key recommendations and providing the organization's top priorities as part of multilateral techno-democratic statecraft strategy for the 21st century. (Center for a New American Security, Common Code: An Alliance Framework for Democratic Technology Policy, October 2020)

The Biden Administration can combat disinformation by pushing for new governmental structures and legislation: Jankowicz recommends that the U.S. create a counter-disinformation czar and a corresponding directorate within the National Security Council. This office would monitor the information ecosystem for threats and coordinate interagency policy responses. Biden should encourage Congress to establish a federal commission for online oversight and transparency. The new administration should consult and learn from allies with decades of disinformation experience while making generational investments in building media and digital literacy programs. Finally, the Biden Administration should bolster public media as an alternative to for-profit news, which has helped drive polarization and distrust of the media in the U.S. (Nina Jankowicz, Foreign Affairs, How To Defeat Disinformation: An Agenda for the Biden Administration, November 2020).

EVENT READOUTS:

Ensuring the integrity of the election required a whole-of-society-approach including investigative agencies, platforms, journalists, civil society groups, and subject area experts, all of whom helped to inform the public and counter the spread of disinformation: Further collaboration will be required to continue addressing threats in the cyber environment. CISA's budget should be nearly doubled and its authority expanded. The old regulatory framework is obsolete; a new regulatory framework must address the taxonomy of cyber threats, ensuring platforms are accountable, including data privacy and protection. The U.S. needs to lead in this regard or else other countries will shape the regulation of the cyber environment for their needs. There needs to be an infusion of IT modernization at the state and local level to address outdated systems, and Congress needs more personnel with a tech background who understand cyber threats and can inform legislators. There must be consequences for companies when they fail to protect consumer data, and for bad actors, foreign and domestic, who attempt to spread disinformation while respecting the hallmark of free speech. (The Aspen Institute Cyber Summit – Inside the 2020 Election, Navigating an Infodemic – From Elections to Vaccines, The View from Capitol Hill, December 2020)

Covid-19 introduces several challenges in the effective administration of elections, including several prominent developments in the employment of disinformation in the pre-electoral environment: Rather than threats originating from foreign state and non-state actors, domestic actors are now using similar tactics to influence electoral outcomes. Because of a lack of a regulatory framework, domestic actors are able to exploit the lack of restrictions to their advantage. The effect is an "arms race," in which domestic actors on either side of an election feel compelled to use similar tactics to achieve their goals. Additionally, there has been a rise in the misappropriation of state resources for electoral gain. The International Foundation for Electoral Systems has identified tools to help counter these challenges to the new electoral environment, but regulatory frameworks must be updated to accommodate these developments. The complexity of various information environments necessitates a multi-stakeholder approach that customizes solutions to address the threats to the integrity of elections. (Virginia Atkinson, Staffan Darnolf, and Lisa Reppel, USC Annenberg Center on Communication Leadership, COVID-19 and Democracy: Global lessons learned on election administration, inclusion, and disinformation, October 2020)

When people experience feelings of uncertainty, anxiety, and helplessness caused by significant events of great consequence that have no immediate explanation, they may turn to conspiracy theories (CTs) as a psychological coping mechanism: CTs help explain political misfortunes for those on the losing side, especially if these people feel helpless; it is easier for them to believe the other side cheated rather than accept that their ideas were rejected. When CTs lead to real world consequences like vaccine refusal and political violence, their spread must be addressed. CTs spread because the business model that drives social media engagement is based primarily on passing on misinformation and should be addressed through platform regulation and algorithm transparency. Attempts at inoculation, like the effort to inform the U.S. public of the delay in tallying the 2020 vote, are helpful, but conspiracy theories will continue to take hold and spread until policy makers can better address the large scale events that cause people to connect to CTs to fulfill their psychological needs. (Dr. Aleksandra Cichocka, Karen Douglas, Jaron Harambam, Joanne Miller PhD,Apolitical, The Infodemic: The Rise of Conspiracy Theories and How Governments Can Respond, December 2020)

To regulate the misinformation crisis the European Union should implement standardized metrics and annual goals monitored by a regulatory authority: The recent fact-checking failures in regard to the U.S. presidential election have caused concerns over the rapid spread of misinformation in the European Union. Various social media outlets are inconsistent in their policies and are not quick enough to label information as false, allowing for a greater impact of disinformation on the population. Additionally, the lack of transparency surrounding fact-checking policies has led the public to believe that the removal of harmful misinformation campaigns is a form of censorship. To tackle the spread of misinformation, social media outlets should be quicker, more transparent, and also provide audiences with the correct information in their approaches to misinformation. (Sarah Andrew, Christoph Schott, EU Disinfo Lab, Regulating Disinformation in the EU - Cautionary Tales from the US Elections, November 2020)

FURTHER READINGS:

Leaks, Lies, and Altered Tape: Russia's Maturing Information Manipulation Playbook
- (Jessica Brandt and Amber Frankland, Alliance for Securing Democracy, October 2020, 30-minute read)

Moscow's Disinformation Offensive During COVID-19: The Case of Lithuania
- (Richard Weitz and Lukas Pieciukaitis, The Hudson Institute, October 2020, 20-min read)

Putin, Putinism, and the Domestic Determinants of Russian Foreign Policy
- (Michael McFaul, *International Security*, October 2020, 45-minute read)

Russian Narratives on Election Fraud
- (Ben Nimmo and the Graphika Team, Election Integrity Partnership, November 2020, 15-min read)

Visualising Influence: Information Bubbles and Ideological Proximities on Czech, Hungarian & Slovak Facebook
- (Miroslava Sawiris, GLOBSEC Policy Institute, October 2020, 30-minute read)

How Journalists Become an Unwitting Cog in the Influence Machine

- (Alicia Wanless, Laura Walters, Carnegie Endowment for International Peace, October 2020, 10-minute read)

Foreign Interference in the 2020 Election

- (William Marcellino, Christian Johnson, Marek N. Posard, Todd C. Helmus, RAND, October 2020, 45-minute read)

Cyber-Enabled Foreign Interference in Elections and Referendums

- (Sarah O'Connor, Fergus Hanson, Emilia Currey, Tracy Beattie, ASPI, October 2020, 30-minute read)

KEY ACADEMIC COUNTER-DISINFO RESOURCES & TOOLS:

Fighting Disinformation Online: A Database of Web Tools, RAND Corporation

Media Well, Social Science Research Council

ComProp Navigator, Oxford Internet Institute, University of Oxford

Hamilton 2.0, Alliance for Securing Democracy, German Marshall Fund

The Debunking Handbook 2020, Center for Climate Change Communication, George Mason University

Please note these summaries of academic research are compiled with the help of students and are for informational purposes only; they do not imply USG endorsement of the views expressed in the articles or their summaries. To receive GEC Academic & Think-Tank Highlights on Countering China's, Iran's, Russia's, and/or Terrorist/Violent Extremist's Propaganda and Disinformation please email (b)(6) @state.gov or visit GEC IQ.

Sender: (b)(6) @state.gov>
Recipient: (b)(6) @america.gov>

UNCLASSIFIED

GEC

ACADEMIC & THINK TANK HIGHLIGHTS
GLOBAL ENGAGEMENT CENTER
December 2020

Dear Readers,
We track close to 100 academic and think-tank sources to bring you GEC's Academic & Think-Tank Highlights. Please click here to take our brief survey to help improve this product and its circulation.
Thank you,
(b)(6)

Please note these summaries of academic research are compiled with the help of students and are for informational purposes only; they do not imply USG endorsement of the views expressed in the articles or their summaries. To receive GEC Academic & Think-Tank Highlights on Countering China's, Iran's, Russia's, and/or Terrorist/Violent Extremist's Propaganda and Disinformation please email (b)(6) *state.gov or visit GEC IQ.*

Countering Russian Disinformation
Academic & Think-Tank Highlights
December 2020

EXECUTIVE SUMMARY: RT uses Soviet-era organizational behavior to produce anti-Western content, pro-Kremlin outlets launder disinformation by intentionally mistranslating foreign media outlets, and the Wagner Group spearheads information operations in Africa. Meanwhile, research indicates that inauthentic Twitter accounts can be identified by an algorithm that assesses only behavioral features. Source labeling and media literacy interventions reduce engagement with Kremlin disinformation. Prior engagement and agreement with fake news may better predict the likelihood of sharing disinformation, and conspiracy theorizing fulfills psychological needs. Additionally, analysis of the U.S. presidential election shows links between domestic and international disinformation framing, reinforces the need for a whole-of-society approach to election integrity, and considers the impact of Covid-19 and Covid-19 misinformation on election administration. Finally, in the policy realm, gaps left by media platforms might be filled by EU regulation and the US could use increased messaging to Russian citizens to achieve a variety of goals.

ACADEMIC/PEER REVIEWED:

The RT news network uses Soviet-era organizational behavior to produce anti-Western content in accordance with the goals of Russian state defense policy: Professional journalistic skills are not prioritized in the hiring process. Following hiring, a socialization process fosters loyalty and conformance to RT's organizational practices. Such practices most prominently include self-censorship and media distortion. Through these methods, RT is able to fulfil three goals: first, to push the idea that Western countries have as many problems as Russia; second, to encourage conspiracy theories about media institutions in the West in order to discredit and delegitimize them; and third, to create controversy about RT, making it appear that the channel is important. (Mona Elswah and Philip N. Howard, Oxford Academic Journal of Communication, "Anything that Causes Chaos": The Organizational Behavior of Russia Today (RT), October 2020)

UNCLASSIFIED

Inauthentic Twitter accounts can be identified by an algorithm that assesses only behavioral features: An algorithm using behavioral rather than linguistic features eliminates the need for language-specific processing and therefore provides more utility. The relevant behavioral features included above-average number of retweets, hashtags, URLs, and replies. Additionally, because inauthentic accounts are operated by state agency employees, activity is higher during weekdays and regular office hours. Identifying inauthentic accounts based solely on behavior can be enriched by considering other behavioral features of employee-run inauthentic accounts and by evaluating behavior-based algorithms against more diverse sets of accounts. (Saleh Alhazbi, IEEE Access, Behavior-Based Machine Learning Approaches to Identify State-Sponsored Trolls on Twitter, November 2020)

Prior familiarity with fake news stories as well as the belief that these stories were likely to be true and aligned with users' pre-existing values consistently predicted the likelihood that users would share disinformation, whereas the measure of digital literacy, authoritativeness of a source, and a posts popularity did not: In contrast to past research on personality and social media behavior, lower levels of agreeableness and higher levels of extraversion are associated with a greater probability of sharing or liking stories. This study implies that interventions are likely to be most effective when targeted at individuals who already hold an opinion or belief, rather than interventions attempting to change people's minds. In addition, repeated exposure of disinformation materials increases the likelihood of sharing them even if users do not believe them. (Tom Buchanan, PLOS ONE, Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation, October 2020)

THINK-TANK ANALYSIS:

Increased messaging to Russian citizens is more symmetrical than a cyber operation, is less likely to spillover to other domains, and can be targeted to achieve a variety of goals: Increasing efforts to communicate directly with Russian citizens "might even add stability to the US-Russian relationship by establishing a balance of information power." Direct forms of communication could be used for several purposes: in case communication needs are urgent, to encourage incremental change, to inflame discontent, as a public diplomacy medium, or to demonstrate American capacity to penetrate Russia's information environment. The US could address Russians directly or work with non-governmental activists. But any strategy "must include alternative technical options" to remain effective in the face of Russian internet shutdowns or censorship efforts. (Thomas Kent, The Jamestown Foundation, US Messaging to Russian Citizens: Time to Step It Up?, November 2020)

Pro-Kremlin outlets launder disinformation by intentionally mistranslating foreign media outlets: Outlets peddling disinformation first identify an article in a respected foreign media outlet on a topic which is related to the narrative that the pro-Kremlin outlet wants to advance. Next, an original Russian-language piece is written that misquotes or misrepresents quotes from

UNCLASSIFIED

the reputable foreign media article, even going so far as to falsify information. The Russian language article is then translated into another language and published in an outlet that appears unrelated to pro-Kremlin outlets. This form of disinformation laundering is difficult to spot because it requires competency in several languages. (EUvsDisinfo, From English into Russian into Czech: Re-Translation as a Manipulative Tool, October 2020)

"Dispatched in dozens of countries, the Wagner Group has been tasked with implementing the Kremlin's foreign policy and deploying aggressive tactics, such as industrial-scale manufacturing of fake news, intimidation of journalists and political opponents, election interference" and more: Russian interests in Africa include lucrative security and mining contracts as well as creating a sphere of influence to direct General Assembly of the United Nations votes in Russia's favor. In addition to conventional soft power initiatives, Russian financial support for the Central African Republic's cash-strapped media sector contributes to its use as a pro-Russia propaganda tool. Counter disinformation efforts will require financial support to substitute for Russian money as well as an acknowledgment of and engagement with high rates of illiteracy. (Nathalia Dukhan, Atlantic Council, Central African Republic: Ground Zero for Russian Influence in Central Africa, October 2020)

Voting-specific narratives of the last presidential election link isolated issues in an attempt to prove that there was a vast conspiracy determining the outcome, and that therefore the outcome is fraudulent: If believed by a large number of Americans, these delegitimization narratives constitute a major concern, however any intervention against domestic disinformation risks being cast as censorship. New platforms like Parler promote their services on the basis of freedom of speech, but because Parler lacks an election integrity team—like those employed by Facebook and Twitter to flag misinformation—their service is easily targeted for monetary and ideological purposes. Disinformation campaigns run continuously both domestically and internationally, but by monitoring social media, false narratives can be identified early enough for fact checkers to limit their impact. (Freeman Spogli Institute for International Studies, Society Needs to Adapt to a World of Widespread Disinformation, October 2020)

In the short term, the U.S. has been slow to adapt to emerging threats from authoritarian states, but can regain advantage in the long term via four spheres of competition: political, economic, technological, and informational: Authoritarians exploit democracies' openness, manipulate information, and penetrate permissive political influence systems, but the U.S. can respond by strengthening key institutions, cultivating civic engagement, and highlighting the corruption and political repression of autocracies. The U.S. must make strategic investments at home—including in infrastructure, education, and basic research—while also supporting innovation and development in key industries. The U.S. should work with other democracies to shape global technology governance to ensure that norms, standards, and new technologies are conducive rather than corrosive to democracy. Trusted information is the foundation of a healthy society, and democracies need to counter threats of authoritarian interference in the information space without compromising the democratic value of free expression. To do so, the United States should embrace media and digital literacy education, ensure that information architecture

UNCLASSIFIED

supports democratic values, challenge authoritarian narrative dominance, and reinvigorate independent journalism. (Alliance for Securing Democracy, Linking Values and Strategy: How Democracies Can Offset Autocratic Advances, October 2020)

THREAT AGNOSTIC:

Source labeling and media literacy interventions reduce engagement with Kremlin disinformation: IREX's Learn to Discern approach revealed several key findings on the effect media literacy messaging could have on social media users. Kremlin propaganda evokes emotional responses, which drives propaganda's rapid spread. However, brief media literacy interventions of only two minutes can shift behaviors of hard-to-reach groups with the strongest effect on partisan news consumers. Labeling propaganda with its source also reduces the likelihood that partisan participants will like/share content, and the two interventions are complementary. The trial results are promising, but further research is required to understand more about specific types of media literacy messages, the audiences they best influence, and the effects of different levels of exposure. (IREX, Randomized Control Trial Finds IREX's Media Literacy Messages to be Effective in Reducing Engagement with Disinformation, October 2020)

The majority of misinformation narratives about the 2020 election originated from domestic actors and have been utilized by foreign state actors and media to sow domestic and foreign distrust in the U.S. political system: After the 2020 presidential election, there has been a strong influx of false and misleading information about the validity of the election results and the integrity of the voting process. The election received large amounts of coverage from Russian and Iranian state media, while Chinese state media accounts provided far less. Russian and Iranian state media served as amplifiers of false and misleading information, often retweeting prominent American outlets or individuals, with a heavy reliance on President Trump's twitter feed to advance claims mentioning "fraud, "rigged" or "steal." China, however, added disclaimers to its retweets, indicating that claims were "unproven" or "unsubstantiated." Each country's amplification of misinformation narratives (or lack thereof) reflects their preferences in information strategies as well as their preferences between the two presidential candidates. Additionally, all three countries have provided significant coverage of unrest and sporadic violence in the U.S., following a pattern of exaggerating the supposed decline of U.S. society. (Bret Schafer, Alliance for Securing Democracy, Foreign Amplification of Voter Fraud Narratives: How Russian, Iranian, and Chinese Messengers Have Leveraged Post-Election Unrest in the United States, November 2020)

A recent study from the UK found that because of current widespread misinformation, there remains high uncertainty regarding public vaccination intentions, and for community protection to be achieved, at least 80% of the community must be vaccinated: In order to overcome this hesitancy and ensure effective coverage is achieved, governments must start an open dialogue with the public regarding vaccine deployment, which is critical to build support about who has vaccination priority, address fears about safety, communicate complex information about multiple vaccines, and counter misinformation and public complacency. The most pressing

UNCLASSIFIED

challenges include making vaccinations convenient by building on existing immunization programs, implementing decentralized local vaccination programs tailored to community needs, adopting transparent principles of vaccination priority groups including sufficient public debate, empowering the public to spot and report misinformation, and ensuring accountability for media companies to remove harmful information and punishing those who spread misinformation. (Melinda Mills, The British Academy, Vaccine Hesitancy Threatens to Undermine Pandemic Response, November 2020)

Technological leadership by the world's major liberal-democratic nations will be essential to safeguarding democratic institutions, norms, and values, and will contribute to global peace and prosperity: Those who shape the use of emerging technologies will garner economic, military, and political strength for decades. A unified approach by like-minded nations is needed to counteract growing investments in and deployments of emerging technologies by authoritarian, revisionist powers. To that end, a technology alliance should be formed; the writers offer a blueprint to move from concept to actionable items, offering a summary of 13 key recommendations and providing the organization's top priorities as part of multilateral techno-democratic statecraft strategy for the 21st century. (Center for a New American Security, Common Code: An Alliance Framework for Democratic Technology Policy, October 2020)

The Biden Administration can combat disinformation by pushing for new governmental structures and legislation: Jankowicz recommends that the U.S. create a counter-disinformation czar and a corresponding directorate within the National Security Council. This office would monitor the information ecosystem for threats and coordinate interagency policy responses. Biden should encourage Congress to establish a federal commission for online oversight and transparency. The new administration should consult and learn from allies with decades of disinformation experience while making generational investments in building media and digital literacy programs. Finally, the Biden Administration should bolster public media as an alternative to for-profit news, which has helped drive polarization and distrust of the media in the U.S. (Nina Jankowicz, Foreign Affairs, How To Defeat Disinformation: An Agenda for the Biden Administration, November 2020).

EVENT READOUTS:

Ensuring the integrity of the election required a whole-of-society-approach including investigative agencies, platforms, journalists, civil society groups, and subject area experts, all of whom helped to inform the public and counter the spread of disinformation: Further collaboration will be required to continue addressing threats in the cyber environment. CISA's budget should be nearly doubled and its authority expanded. The old regulatory framework is obsolete; a new regulatory framework must address the taxonomy of cyber threats, ensuring platforms are accountable, including data privacy and protection. The U.S. needs to lead in this regard or else other countries will shape the regulation of the cyber environment for their needs. There needs to be an infusion of IT modernization at the state and local level to address outdated systems, and Congress needs more personnel with a tech background who understand cyber

UNCLASSIFIED

threats and can inform legislators. There must be consequences for companies when they fail to protect consumer data, and for bad actors, foreign and domestic, who attempt to spread disinformation while respecting the hallmark of free speech. (The Aspen Institute Cyber Summit – Inside the 2020 Election, Navigating an Infodemic – From Elections to Vaccines, The View from Capitol Hill, December 2020)

Covid-19 introduces several challenges in the effective administration of elections, including several prominent developments in the employment of disinformation in the pre-electoral environment: Rather than threats originating from foreign state and non-state actors, domestic actors are now using similar tactics to influence electoral outcomes. Because of a lack of a regulatory framework, domestic actors are able to exploit the lack of restrictions to their advantage. The effect is an "arms race," in which domestic actors on either side of an election feel compelled to use similar tactics to achieve their goals. Additionally, there has been a rise in the misappropriation of state resources for electoral gain. The International Foundation for Electoral Systems has identified tools to help counter these challenges to the new electoral environment, but regulatory frameworks must be updated to accommodate these developments. The complexity of various information environments necessitates a multi-stakeholder approach that customizes solutions to address the threats to the integrity of elections. (Virginia Atkinson, Staffan Darnolf, and Lisa Reppel, USC Annenberg Center on Communication Leadership, COVID-19 and Democracy: Global lessons learned on election administration, inclusion, and disinformation, October 2020)

When people experience feelings of uncertainty, anxiety, and helplessness caused by significant events of great consequence that have no immediate explanation, they may turn to conspiracy theories (CTs) as a psychological coping mechanism: CTs help explain political misfortunes for those on the losing side, especially if these people feel helpless; it is easier for them to believe the other side cheated rather than accept that their ideas were rejected. When CTs lead to real world consequences like vaccine refusal and political violence, their spread must be addressed. CTs spread because the business model that drives social media engagement is based primarily on passing on misinformation and should be addressed through platform regulation and algorithm transparency. Attempts at inoculation, like the effort to inform the U.S. public of the delay in tallying the 2020 vote, are helpful, but conspiracy theories will continue to take hold and spread until policy makers can better address the large scale events that cause people to connect to CTs to fulfill their psychological needs. (Dr. Aleksandra Cichocka, Karen Douglas, Jaron Harambam, Joanne Miller PhD, Apolitical, The Infodemic: The Rise of Conspiracy Theories and How Governments Can Respond, December 2020)

To regulate the misinformation crisis the European Union should implement standardized metrics and annual goals monitored by a regulatory authority: The recent fact-checking failures in regard to the U.S. presidential election have caused concerns over the rapid spread of misinformation in the European Union. Various social media outlets are inconsistent in their policies and are not quick enough to label information as false, allowing for a greater impact of disinformation on the population. Additionally, the lack of transparency surrounding fact-

UNCLASSIFIED

checking policies has led the public to believe that the removal of harmful misinformation campaigns is a form of censorship. To tackle the spread of misinformation, social media outlets should be quicker, more transparent, and also provide audiences with the correct information in their approaches to misinformation. (Sarah Andrew, Christoph Schott, EU Disinfo Lab, Regulating Disinformation in the EU - Cautionary Tales from the US Elections, November 2020)

FURTHER READINGS:

Leaks, Lies, and Altered Tape: Russia's Maturing Information Manipulation Playbook
- (Jessica Brandt and Amber Frankland, Alliance for Securing Democracy, October 2020, 30-minute read)

Moscow's Disinformation Offensive During COVID-19: The Case of Lithuania
- (Richard Weitz and Lukas Pieciukaitis, The Hudson Institute, October 2020, 20-min read)

Putin, Putinism, and the Domestic Determinants of Russian Foreign Policy
- (Michael McFaul, *International Security*, October 2020, 45-minute read)

Russian Narratives on Election Fraud
- (Ben Nimmo and the Graphika Team, Election Integrity Partnership, November 2020, 15-min read)

Visualising Influence: Information Bubbles and Ideological Proximities on Czech, Hungarian & Slovak Facebook
- (Miroslava Sawiris, GLOBSEC Policy Institute, October 2020, 30-minute read)

How Journalists Become an Unwitting Cog in the Influence Machine
- (Alicia Wanless, Laura Walters, Carnegie Endowment for International Peace, October 2020, 10-minute read)

Foreign Interference in the 2020 Election
- (William Marcellino, Christian Johnson, Marek N. Posard, Todd C. Helmus, RAND, October 2020, 45-minute read)

Cyber-Enabled Foreign Interference in Elections and Referendums
- (Sarah O'Connor, Fergus Hanson, Emilia Currey, Tracy Beattie, ASPI, October 2020, 30-minute read)

KEY ACADEMIC COUNTER-DISINFO RESOURCES & TOOLS:

Fighting Disinformation Online: A Database of Web Tools, RAND Corporation

Media Well, Social Science Research Council

ComProp Navigator, Oxford Internet Institute, University of Oxford

Hamilton 2.0, Alliance for Securing Democracy, German Marshall Fund

UNCLASSIFIED

GEC

ACADEMIC & THINK TANK HIGHLIGHTS
GLOBAL ENGAGEMENT CENTER
December 2020

The Debunking Handbook 2020, Center for Climate Change Communication, George Mason University

Please note these summaries of academic research are compiled with the help of students and are for informational purposes only; they do not imply USG endorsement of the views expressed in the articles or their summaries. To receive GEC Academic & Think-Tank Highlights on Countering China's, Iran's, Russia's, and/or Terrorist/Violent Extremist's Propaganda and Disinformation please email [redacted]@state.gov or visit GEC IQ.

(b)(6)

From: (b)(6) @state.gov>
To: (b)(6) @state.gov>
CC: (b)(6) @state.gov>
Subject: FW: Debunk EU: Disinformation tsunami against the Baltic states during Belarus protests
Date: Fri, 2 Oct 2020 21:01:39 +0000

Hi (b)(6)

Great to meet you over WebEx earlier this week and talk about GEC programs. I received this product yesterday from a Lithuanian NGO that receives GEC funding – the attachment here concerns some disinformation research they have done in the Baltics.

Best,
(b)(6)

From: Viktoras Daukšas | Debunk EU (b)(6) @debunkeu.org>
Sent: Thursday, October 1, 2020 3:36 AM
Subject: Debunk EU: Disinformation tsunami against the Baltic states during Belarus protests

Hi,

Here is the new report from Debunk EU: Lithuania, Latvia, and Estonia disinformation analysis for August 2020.

During the month of August, we have managed to analyse 6500 content pieces throughout all three countries.

The events in Belarus, where people are protesting after the implicit falsification of the results of presidential election, were topical in the media agenda-setting in August. Therefore, it is not surprising that the pro-Kremlin propaganda actively used this topic too. In its own narratives about Belarus, it reserved special places for the Baltic states (especially for Lithuania). The Baltic states, together with other regional countries, were presented as the provokers of the protests.
Read full article:
https://medium.com/@DebunkEU/debunk-eu-election-fraud-in-belarus-brought-a-surge-of-pro-kremlin-propaganda-e41a350ed7f9

The report is attached as PDF.

About Debunk EU
Debunk EU, VsI, is an independent technology think tank and non-governmental organisation that researches disinformation and runs educational media literacy campaigns. Debunk EU conducts

disinformation analysis in the Baltic states, as well as in the United States and Northern Macedonia together with the partners.
Debunk EU was noticed by such media giants as “The Financial Times” and “Deutsche Welle”. The organisation has presented its activities in 17 countries, including the United States, Germany, the United Kingdom, France, Serbia, etc.

Published reports:

https://medium.com/@DebunkEU

Social media:

https://www.facebook.com/DebunkEU

https://www.linkedin.com/company/debunk-eu/

https://twitter.com/DebunkEu

--
--
Viktoras Daukšas
Head of Debunk EU
Mob. tel. (b)(6)
https://www.linkedin.com/in/viktorasdauksas

Sender: (b)(6) @state.gov>

Recipient: state.gov>; @state.gov>

From: (b)(6)
To: @state.gov>
Subject: Chat conversation with (b)(6) from Microsoft Teams
Date: Mon, 23 Jan 2023 15:52:37 +0000

Microsoft Teams

(b)(6) 6 months ago
(b)(5)

Sender: (b)(6)
Recipient: @state.gov>

From: (b)(6)
To: (b)(6) state.gov>
Subject: Chat conversation with (b)(6) from Microsoft Teams
Date: Mon, 23 Jan 2023 17:07:03 +0000

Microsoft Teams

(b)(6) 2 months ago
(b)(5)

Sender: (b)(6)
Recipient: (b)(6) state.gov>

Special Envoy Gabrielle's Remarks for the Hybrid Threats to Democracy Panel
Globsec Bratislava 2020 Forum
Video Conference Call (HST 2426)
October 7, 09:55-10:55am EST

(U) EVENT DESCRIPTION

You have accepted the Globsec invitation to participate as panelist speaker at its "Globsec Bratislava 2020 Forum" on the panel focused on the topic of "Hybrid Threats to Democracy". The panel will be one hour in duration. The format of the panel has been updated to a "discussion" around questions directed to the panelists. The moderator will introduce you and pose the question "How does the GEC counter disinformation and propaganda, what approach would you recommend for societies to address disinformation and propaganda?" At this point, you will deliver introductory remarks. Following this, the moderator will ask topical questions to the panelists. The questions directed to you will be selected from the Q&A below. Around 200-300 participants are expected in-person and the panel will be available virtually for all attendees. The Forum is a two-day event and you are slated to speak on the first day.

~~(SBU)~~ LAST MEETING: You last interacted with Globsec leadership when you attended the Globsec Bratislava 2019 Forum and provided remarks during the 2019 European tour with former GEC Russia Director (b)(6) During this trip, you also attended the Globsec International Advisory Board Meeting and built a rapport with Globsec's team led by (b)(6) who works closely with the GEC in our cooperative agreement.

(U) PANELISTS (BIOGRAPHIES IN TAB 3)

GEC Special Envoy Lea Gabrielle

Dr. Teija Tiilikainen

Director, European Centre of Excellence for Countering Hybrid Threats, Helsinki

Former Secretary of State at the Ministry for Foreign Affairs of Finland

Ms. Veka Modebadze, LLM

Director, Strategic Communications Department, Georgia Ministry of Foreign Affairs

Dr. Jyun-Yi Li

Associate Researcher at the Institute for National Defense and Security Research

Ms. Katarina Klingova

Senior Research Fellow, Democracy & Resilience, GLOBSEC Policy Institute

Ms. Annabelle Chapman

(Moderator) Freelance Journalist Correspondent Warsaw

(b)(5)

(U) KEY OBJECTIVES

1. [redacted]
2. Answer the questions put forward to the panel:
   a. How should democratic societies react to a rapidly shifting threat horizon and the increasingly difficult attribution of threat originators?
   b. What should be done to boost EU and NATO capacities to detect and deter hybrid threats?

 (b)(5)

c. How should strategic communication be mainstreamed into every aspect of modern foreign and security policy measures?

3. [redacted]

BACKGROUND :

Globsec Forum

(U) Hosted by the Slovak think tank Globsec, the Globsec Forum has established itself as the leading platform for strategic security discussion in the Central and Eastern European region and one of the top strategic conferences globally. The conference brings together more than 1,000 key stakeholders from more than 65 countries, including state officials, business leaders, experts from leading global think tanks and NGOs, heads of international organizations, and security professionals in Europe. Held in Slovakia every year, the conference usually hosts key European political and diplomatic leaders. Due to COVID-19, the conference will be making virtual accommodations for the first time.

(U) The Globsec Bratislava 2020 Forum will address five key topics in the future of security and strategy: Defense and Security, Digital Future, Sustainability, Future of Europe, and the Economy and Global Order. Aligned to these topics, leaders will discuss emerging threats facing European states and global partners and the solutions available to mitigate and counter these threats. The Special Envoy has been invited to provide remarks at the Hybrid Threats to Democracy Panel. This panel will provide key insights on emerging hybrid threats including how narratives and the flow of information are critical components of modern security issues. COVID-19 and the global response to the pandemic highlight the importance of how narratives can be shaped to assist or interfere in conditions that threaten a society.

Slovakia

(SBU) Prime Minister Igor Matovic's OLaNO party won the February 29 parliamentary election, unseating the ruling Smer-SD government. The new government's approved platform is pro-reform and pro-Western, with a stated focus on anti-corruption and rule of law. Much of the political turnover is the result of calls for political reform following the murder of journalist Jan Kuciak and his fiancée Martina Kusnirova. On August 10, the Ministry of Foreign and European Affairs (MFEA) expelled three Russian diplomats, likely in relation to the murder of a former Chechen rebel in Berlin in 2019. (b)(5) (b)(5) (b)(5) (b)(5) (b)(5) Despite the government's pro-Western stance, a Globsec survey conducted in March shows half of Slovaks feel threatened by "Western" values and 53 percent identify the United States specifically as a danger. By comparison, in Central Europe these sentiments are only 28 percent. Additionally, only 26 percent of Slovaks see a similar risk coming from Russia. With a supportive government, and a population vulnerable to Russian malign influence, conditions in Slovakia continue to demonstrate the need to counter Russian disinformation and propaganda activities.

GEC Russia Team Projects in Slovakia:

- (b)(5); (b)(6) [redacted]

- (U) Globsec: The GEC, with DOD SOLIC/SOCT, has provided a $3,000,000 cooperative agreement to Globsec to use innovative research methodology to assess the disinformation landscape of Poland, Czechia, Slovakia, Hungary, Romania, Serbia, Bulgaria, Montenegro, and North Macedonia. This project uses both advanced technical methodology with Graphika to map the online information environment and identify disinformation networks, and on-the-ground polling among populations identified as vulnerable to assess the true effectiveness of targeted Russian disinformation narratives. This project will produce a set of confidential reports to key stakeholders that provide deep details on disinformation networks and vulnerable audiences, and a set of public reports that provide the broad findings of this research for public consumption. A segment of the GEC award budget is dedicated to the 2019 and 2020 Globsec Forums.

- ~~(SBU/FOUO)~~ Upcoming Globsec Funding: With support from Embassy Bratislava, Globsec has applied for a grant through the Annual Program Statement to assist the Slovak government with a Whole-of-Government (WoG) and Whole-of-Society (WoS) approach to countering disinformation. Globsec has not been notified of selection, but the GEC Russia Threat Directorate intends to fund this award with early release funds in December 2020 or January 2021. This project will build on the success of RSP Slovakia to build a sustainable relationship with the Slovak government and to build resiliency against Russian disinformation and propaganda targeting Slovak society and politics.

- ~~(SBU/FOUO)~~ As a part of a wider media literacy training that supports the Visegrad, Black Sea, Baltics, and Balkans regions, the (b)(6) train-the-trainer program offers training in counter disinformation and propaganda available to participants in (b)(6).

- ~~(SBU/FOUO)~~ The GEC previously provided $125,000 in support of Emb. Bratislava's 1989 campaign.

Event Details:

Location: The event is entirely virtual and will take place over XLAB Realtime with vMix connection. The Special Envoy will use the GEC studio for the panel.

Preparation Session: Monday, October 5, 2020 at 1:00pm

Media Exposure: Public

Marketing: The Globsec Fornm is a popnlar European security conference and has been advertised to members of European governments, think tanks, civil society, academics and journalists. The full speaker list is shared with participants and attendees.

Audience: 250-300 participants in the Globsec conference may attend the panel in person. Virtually the panel will be broadcast online publicly.

Recording: The panel will be recorded and played live through a virtual conference.

Attachments:

Tab 1 – TPs for Globsec 2020

Tab 2 – Q&A Globsec 2020

Tab 3 – Panelist Biographies

(b)(6) roved: R/GEC/PDC: Daniel Kimmage (OK)

(b)(6) ted: GEC Russia Team -

GEC Russia Team – (b)(6)

(b)(6) GEC Russia Team -

(b)(6) red: R/GEC/DCS (OK)

(b)(6) R/GEC/DCO: Leah Bray (OK)

(b)(6) R/GEC/PA: (OK)

(b)(6) R/GEC Russia Team: (OK)

(b)(6) R/GEC China Team: (OK)

(b)(6) R/GEC TET: (OK)

(b)(6) R/GEC A&R: (OK)

(b)(6) EUR/RUS: (OK)

(b)(6) EUR/PPD: (OK)

(b)(6) Embassy Bratislava (OK)

(b)(6) EAP/PD: (OK)

(b)(6) EAP/ POL (INFO)

EAP/CM: (OK)

E (OK)

Tab 1 - Talking Points (Anticipated 10 minute remarks):

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

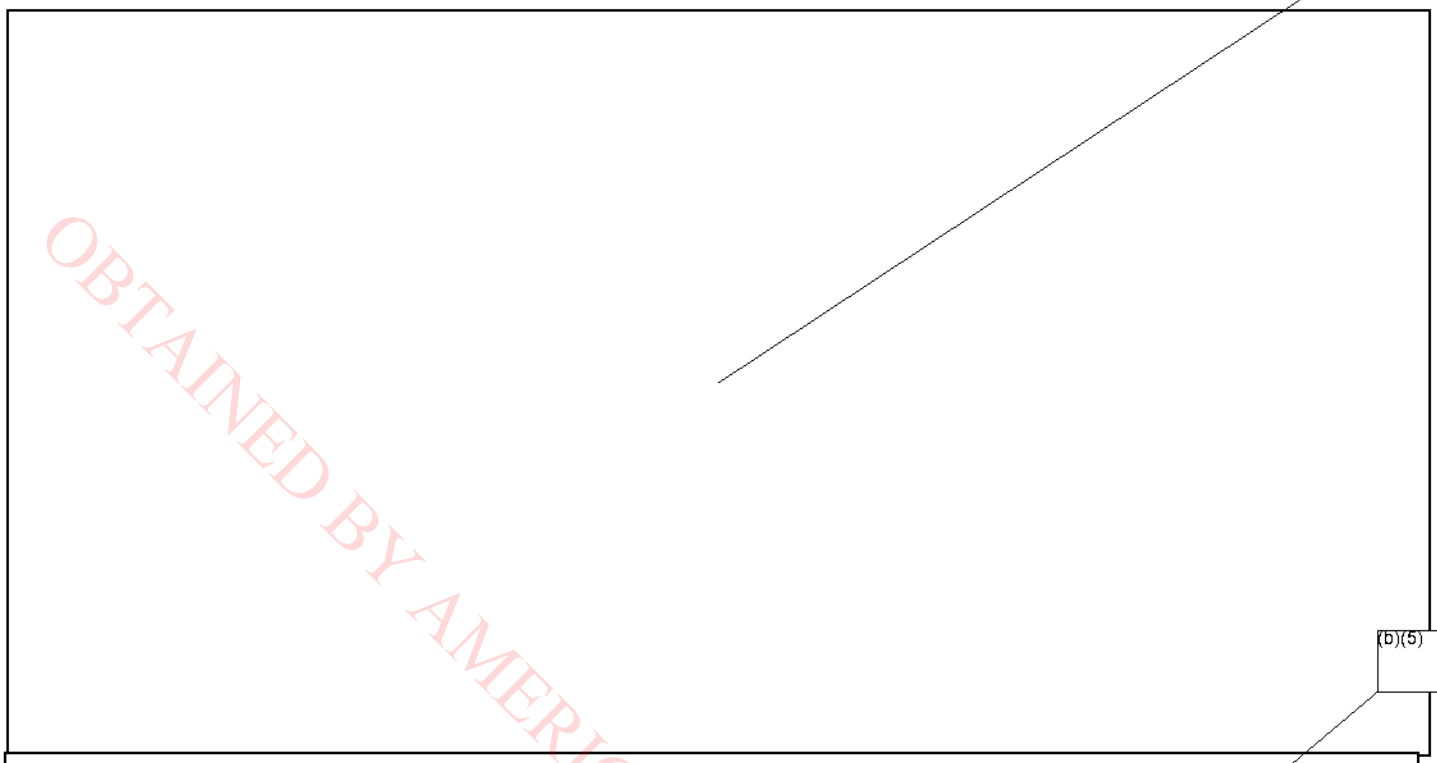
(b)(5)

(b)(5)

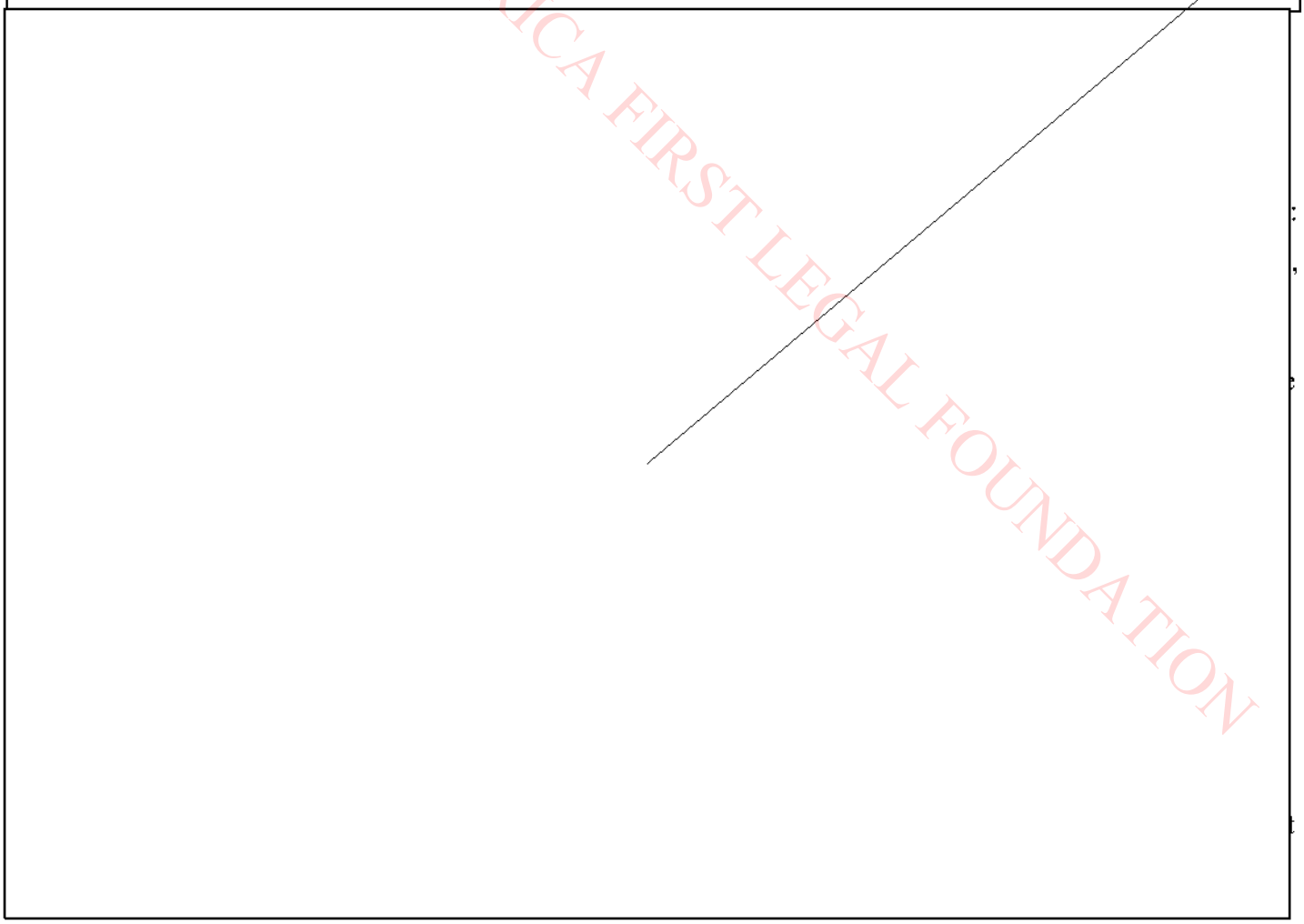
(b)(5)

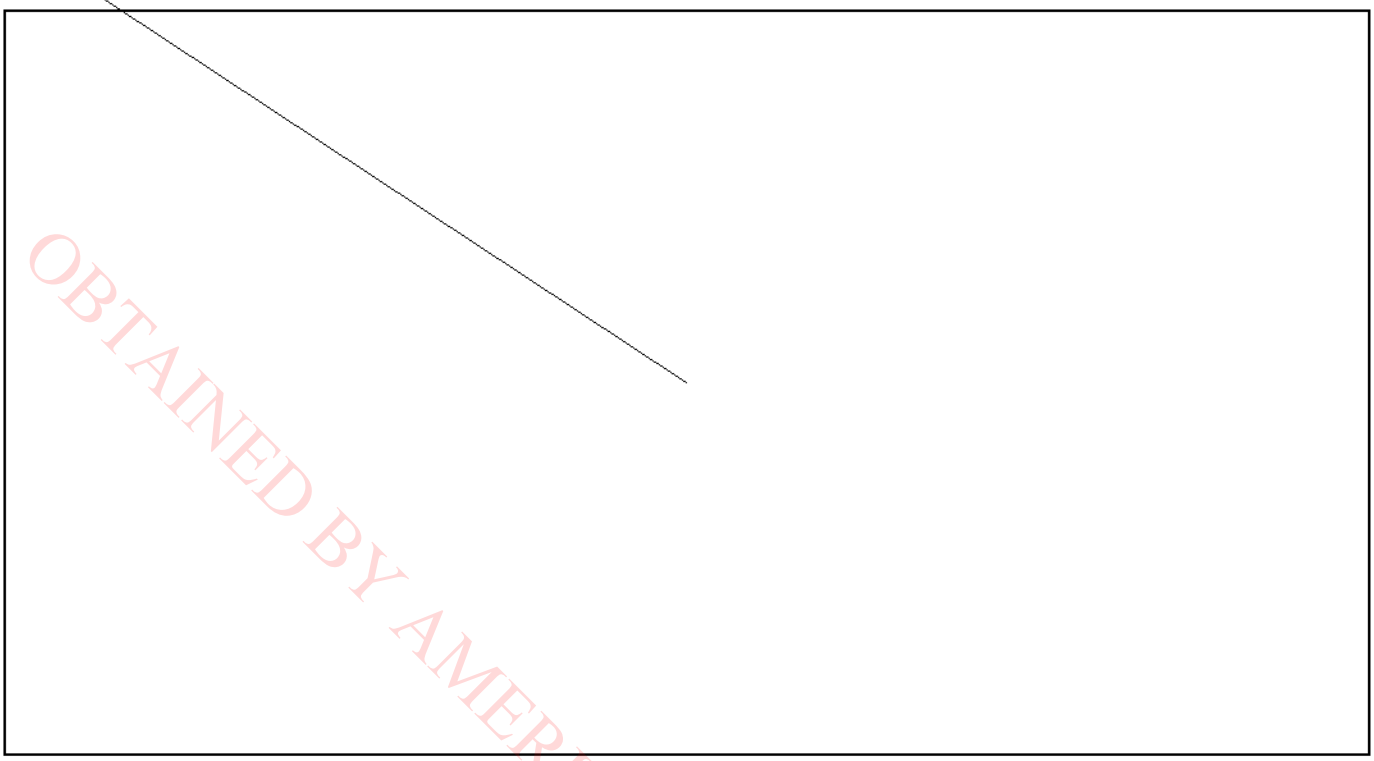
(b)(5)

(b)(5)



(b)(5)





Tab 2 - Q&A Panel: Hybrid Threats to Democracy – "Let's Heal Together"

(b)(5)

Topic: Disinformation and Elections

(b)(5)

(b)(5)

(b)(5)

Topic: Pillars and Ecosystem

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Topic: Social Media

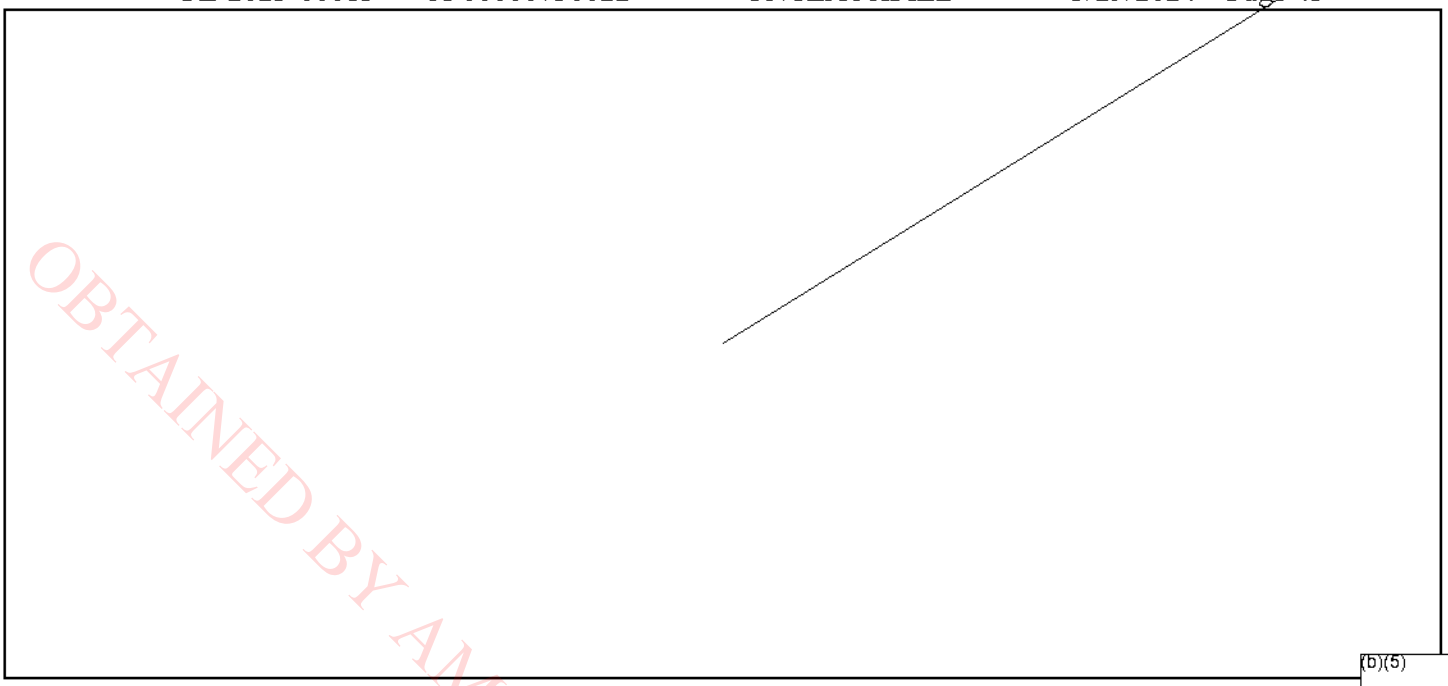
(b)(5)

(b)(5)

(b)(5)

Topic: China Russia Convergence

(b)(5)



(b)(5)

Topic: Huawei

Topic: Taiwan

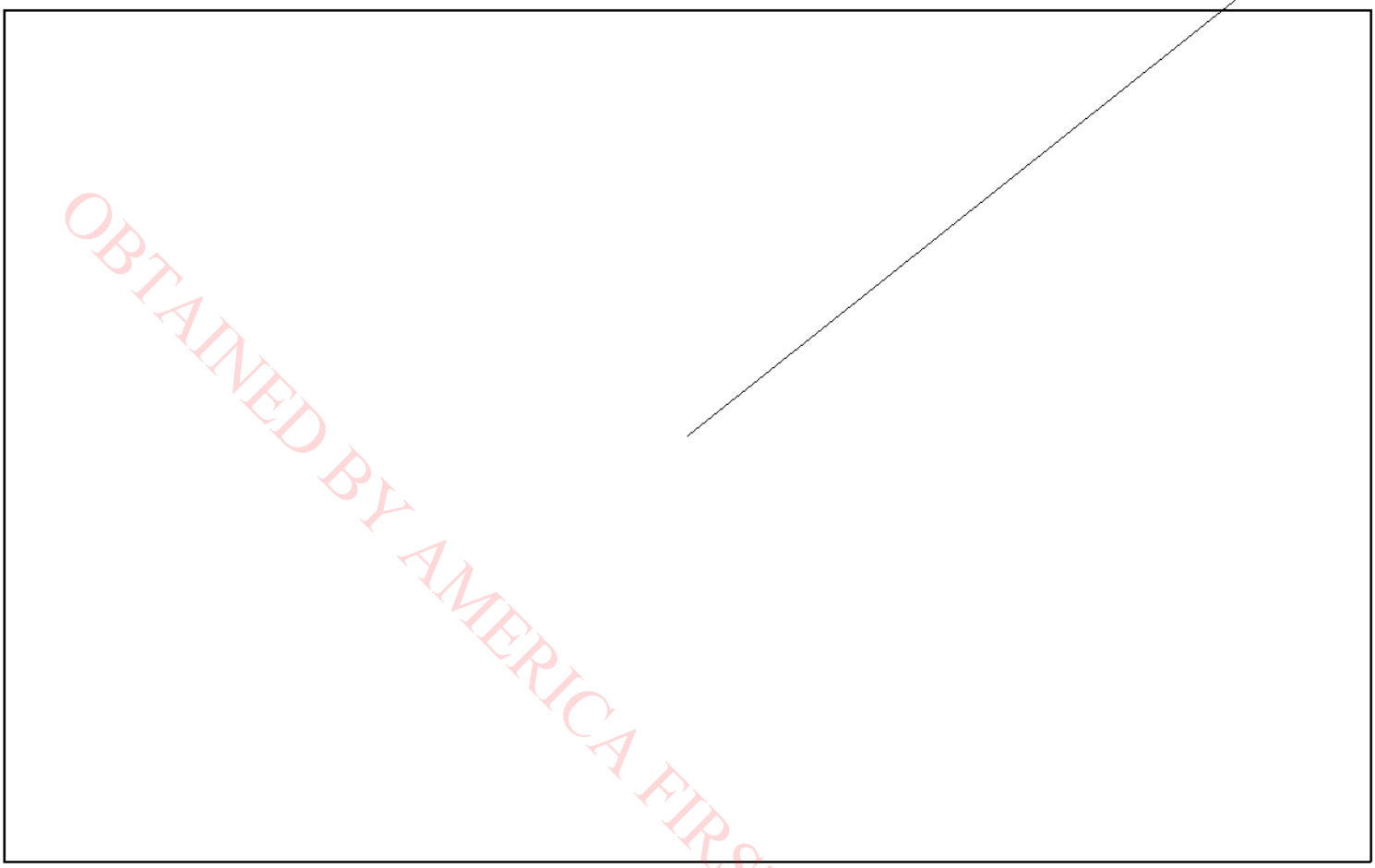
(b)(5)

(U) Taiwan Disinformation

(b)(5)

(SBU) What the GEC is Doing

(b)(5)



Tab 4 -PARTICIPANT BIOGRAPHIES

Dr. Teija Tiilikainen

Director, European Centre of Excellence for Countering Hybrid Threats, Helsinki

Former Secretary of State at the Ministry for Foreign Affairs of Finland

In August 2019, Dr. Teija Tiilikainen was appointed Director of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) for a five-year term.

Dr Tiilikainen is currently the Director of the Finnish Institute of International Affairs (FIIA). Before her appointment to this position in 2010, she was the Director of the Network of European Studies at the University of Helsinki (2003–2009). Dr Tiilikainen has also served as Secretary of State at the Ministry for Foreign Affairs of Finland from 2007 to 2008.

She was a member of the European Convention in 2002-03 and a member of the Panel of Eminent Persons on European Security as a Common Project led by Ambassador Wolfgang Ischinger in 2015-16. In 2018, Dr Tiilikainen was nominated part-time professor (non-residential) at the European University Institute (School of Transnational Governance) in Florence. She is currently the vice-chair of the executive board of the University of Helsinki.

In her research, Dr Tiilikainen has focused on issues related to European integration (institutional questions, the EU's external relations, including Common Foreign and Security Policy and Common Security and Defence Policy) and on European security policy.

Ms. Veka Modebadze, LLM

Director, Strategic Communications Department, Georgia Ministry of Foreign Affairs

Ms. Modebadze is the current Director of the Strategic Communications Department. Prior to her current position, she served as the Head of the Euro-Atlantic Division in the Ministry of Internal Affairs of Georgia. She is also a lecturer on EU Law at the Georgian Institute of Public Affairs (GIPA). Veka has a law degree from Tbilisi State University and an LLM from the College of Europe. During her time at the MFA, she was part of the Professional Fellows Program through the American Councils of the U.S. Department of State.

Dr. Jyun-Yi Lee

Associate Researcher of the Institute for National Defense and Security Research (INDSR)

Dr. Jyun-yi Lee is an Assistant Research Fellow and Acting Director of the Division of Non-traditional Security and Military Mission at the Institute for National Defense and Security Research, Taiwan. He was an assistant research fellow in the Science and Technology Policy Research and Information Center of the National Applied Research Laboratories, Taiwan. He was an assistant professor in the Institute of Strategic and International Affairs at the National Chung Cheng University. Dr. Lee earned his Ph. D. in international relations from University of East Anglia, U K. **INDSR has an ongoing grant with GEC's China Threat Directorate.**

Ms. Katarina Klingova

Senior Research Fellow, Democracy & Resilience, GLOBSEC Policy Institute, Bratislava

Katarína is a senior research fellow at the GLOBSEC Policy Institute, a think tank based in Bratislava. As member of GLOBSEC's Strategic Communication program she has been monitoring disinformation in Slovakia and Central European region since 2016. She has authored or co-authored numerous scholarly analyses on foreign disinformation and subversion in Central Europe, including Vulnerability Index: Subversive Russian Influence in Central Europe and Countering Information Warfare – Lessons Learned from NATO Members and Partner Countries.

MS. ANNABELLE CHAPMAN (MODERATOR)

Freelance Journalist, Warsaw

Ms. Annabelle Chapman is a freelance journalist based in Warsaw, Poland. She writes about Central and Eastern Europe for a range of international publications. Ms. Chapman's articles as a Warsaw correspondent are featured in The Economist (here), Foreign Policy (here), Politico (here) and Monocle (here). Ms. Chapman has won the inaugural Timothy Garton Ash prize for European writing.