Public-Private Partnership on Malign Foreign Influence - Observations & Recommendations

2022 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

I. Executive Summary

There exists a gap between the public and private sectors when it comes to specifically dealing with Malign Foreign Influence (MFI). In researching current examples of success for this issue specifically but also more broadly between the public and private sectors, this team identified a number of important recommendations to provide a model mechanism for partnership, information sharing, and tackling this challenge collaboratively. Among these recommendations is the need for direct engagement with social and digital media companies within the public sector in order to facilitate ongoing communication about disinformation trends, foreign malign influence actors, and ways to counter MFI. Effective coordination across civil society, government agencies, and think tanks to collect the broadest evidence available of MFI to provide for the greatest likelihood of inoculating the public against disinformation campaigns. Significant monetary and resource investment by the government is critical for the success of the public-private partnership project. Finally, enhancing information sharing with private sector entities and ensuring the relevancy of that information for each company will enable a more tailored approach to tackling the issue of MFI across a larger cross section of the private sector.

Homeland Security

II. Key Points

Between the researched models of success for public-private partnerships and the limited responses the team received from both the public and private sectors, our team hopes to offer the Foreign Malign Influence Center unique insight to contribute to the creation of a potential roadmap for its own success in this arena. Among the most critical recommendations provided are the following:

1. Direct engagement with social and digital media companies to communicate about disinformation and better ways to counter it
2. Effective coordination across civil society, government, and think tanks to collect the broadest evidence of MFI taking place
3. Significant government investment into the public-private partnership project
4. Significant buy-in from the private sector for networking and relationship building
5. Direct access to U.S. government resources such as information-sharing
6. FMIC's potential role as an interlocutor between the public and private sectors on disinformation and countering malign foreign influence
7. Assist in establishing training for private and public workforces to identify and counter disinformation and to increase disinformation awareness
8. Identifying key points of contact for the private sector in the U.S. intelligence community for engagement and information sharing in a more structured way
9. Facilitating conferences and seminars between the U.S. intelligence community and the private sector for more direct engagement on the issue of MFI
10. Regulating ongoing direct communication with the private sector on rising trends and current MFI campaigns
11. Enhancing information sharing with private sector entities by tailoring the relevancy of the information being provided to each company specifically

2022 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Team Members

MEMBERS	COMPANY/AGENCY
Champion: Dana LaFon	NSA
Champion: Trisha Ripley	ODNI
Alexandra Armstrong	American Express
Michael Ficht	FBI
Wesley Moy	Johns Hopkins University
Darrell Hall	Department of Health and Human Services
Taylor Price	Dell Technologies
Janice R.	Department of Defense
Eric Schorr	Snap Inc.
Christine Sublett	Sublett Consulting, LLC.
Kimberly Young	DHS/I&A

Homeland Security

III. Introduction

The Public-Private Analytic Exchange Program (AEP), sponsored by the Department of Homeland Security's Office of Intelligence and Analysis (DHS/I&A), on behalf of the Office of the Director of National Intelligence (ODNI), facilitates collaborative partnerships between members of the private sector and teams of experienced U.S. government analysts to form a number of topics committees. This annual program provides U.S. government analysts and private sector partners with a better understanding of select national security and homeland security issues.

The topic committee for *Countering Foreign Malign Social Network Manipulation in the Homeland* has recognized that there exists a gap between the public and private sectors when it comes to specifically dealing with Malign Foreign Influence (MFI). This gap is also recognized in a call for a *Whole of Society* solution to countering MFI, where experts include the broader tech sector as partners to regulate against misinformation campaigns across internet platforms; however, a solution for bridging this gap is not yet offered.

In an attempt to help bridge this gap, this team identified significant public and private industry sectors (i.e., ODNI's Foreign Malign Influence Center and technology) that are impacted by MFI with the goal of examining the public/private industry gaps that hamper solutions to this problem. The team conducted systematic semi-structured interviews and examined successful models of public/private industry partnerships. The team then combined the interview results with ideal models of partnership in order to provide a model mechanism for partnership, information sharing, and tackling this challenge collaboratively.

IV. Model Mechanisms for Private-Public Partnering

IV (a). European Models of Success

While the United States is in the process of establishing the Office of the Director of National Intelligence's (ODNI) Foreign Malign Influence Center (FMIC) and has a variety of entities across the U.S. government addressing disinformation in specific spheres, some foreign governments have already attempted, or are presently attempting, to establish their own organizations in an effort to counter the ever-increasing presence of disinformation. While most countries recognize the threat of disinformation, the governments of Sweden, Czech Republic, France, and the broader European Union (EU) have attempted to establish either independent organizations or branches of existing government agencies to address the threat of disinformation. In all cases, these entities were established in countries or, in the EU's case, regions, with established democratic norms and respect for free speech and expression reflective of the U.S.'s own situation. While none of the examples already established, or in the process of being established, are necessarily ideal, they all provide lessons learned as the FMIC is under development.

In 2017, the Czech Republic (also known as Czechia) which was one of Russia's priority targets for disinformation, established the Center Against Terrorism and Hybrid Threats (CTHT).[12] The CTHT, which was placed within the Czechia Ministry of Interior, would have its work "enhanced" by reporting from the Czech Security Information Service (BIS), civil society organizations, and think tanks. From the beginning, the CTHT faced significant pushback from within its own government, most prominently the President of Czechia at the time, Milos Zeman, as well as a significant minority of the Czech Chamber of Deputies, who all expressed strong sympathies for the Russian government or leadership.[3] Despite the challenges CTHT faced from its origination, it has developed a variety of procedures and actions to help counter disinformation internally and to coordinate with foreign partners. "…the CTHT has managed to produce a variety of analytical documents, proposals for policy measures, and communication outputs for different ministries of the Czech government." In addition to these measures, the CTHT trains civil servants in the government in ways to identify disinformation and how to counter it. Finally, CTHT is reported to communicate with EU entities as well as within Czechia, in order to coordinate on intelligence and policy matters.[4] CTHT's ability to coordinate with EU entities is particularly important, considering the EU has its own series of organizations and entities focused on countering disinformation.

Following Ukraine's Maidan Revolution in February 2014 and Russia's subsequent occupation of Crimea and invasion of eastern Ukraine, the EU recognized that, among other things, they needed to develop ways to better coordinate in countering Russian disinformation, as they witnessed waves of disinformation flow over their populace via social media, television, and radio from Russian actors. Out of this, the EU established the East Stratcom Task Force, established under the EU's diplomatic service, the European External Action Service (EEAS), and it was mandated to address disinformation emanating from Russia. The Task Force developed three separate foci of its work including: improving the

EU's communications, particularly in Eastern Europe and Ukraine; strengthening and enhancing free and independent media organizations in Eastern Europe and Ukraine; and developing an advocacy campaign to raise awareness about disinformation, to include establishing a website, "EUvsDisinfo", to directly challenge Russian disinformation narratives.[5] Additionally, since 2015, the EU has expanded this initiative to also counter Chinese disinformation efforts, conducting data analysis of disinformation, and organizing conferences to discuss disinformation by state actors.[6] The EU has also developed a variety of other responses to counter disinformation at the multinational level, such as developing a Code of Practice to address disinformation online platforms to which key social companies such as Meta and Twitter have signed.[7] The East Stratcom Task Force is intended to be the EU mechanism to coordinate efforts to share information about disinformation and develop methods and practices to counter it.

In addition to relatively more established organizations in Czechia and at the EU level, both Sweden and France have established their own organizations in the past year to attempt to address disinformation at the state level. In October 2021, France established the "Agency for Vigilance and Protection Against Foreign Digital Interference", whose stated purpose is to "…monitor, detect and analyze the operations and techniques of foreign actors to disseminate and amplify online content hostile to France in order to harm the interests of the Nation."[8] Viginum also was established with an ethics committee to review Viginum's actions and ensure it respected France's constitution. However, unlike some other countries, Viginum is not responsible for responding to disinformation or influence operations, but rather to refer them to the French government for further action.[9] Even more recently, in January 2022, Sweden established the Swedish Psychological Defense Agency to protect "democratic society" and "free formation of opinion."[10] In contrast to Viginum, the Psychological Defense Agency intends to work with the Swedish military and government counter disinformation, and will focus solely on foreign actors, not those within Sweden.[11] However, there remain few details about how the organization intends to go about identifying disinformation, or how it intends to communicate their findings to the public. While both France and Sweden's organizations remain incredibly young, if they prove successful in effectively identifying and providing the public evidence of disinformation and countering it, it is likely other countries in the EU, and elsewhere, may attempt to also establish their own state-level entities.

IV (b). OSAC as a Model of Success

The Foreign Malign Influence Center (FMIC) may also find inspiration and guidance for future collaboration and engagement with the U.S. private sector by looking internally in the U.S. government to the State Department, where its own public-private partnership has become a model for success over the last few decades.

The Overseas Security Advisory Council or OSAC was created in 1985 under the Federal Advisory Committee Act with the mission of promoting security cooperation between U.S. private sector companies around the world and the U.S. Department of State.[12] Specifically:

> "OSAC connects private-sector security professionals with the Diplomatic Security Service through ongoing risk awareness and crisis support, analysis and benchmarking, threat mitigation and management training, and by building trusted networks of support through its peer membership groups and year-round social events."[13]

According to OSAC, this partnership currently supports thousands of U.S. companies and organizations with overseas interests or physical presence.[14] Membership in OSAC is free, and open to any corporate, non-profit, academic, faith-based, or other U.S.-incorporated organization of any size with operations outside the United States.[15]

In a case study for ASIS International's Security Management, authors Diana Concannon and Michael Center note that OSAC has demonstrated three critical characteristics necessary for successful public-private partnerships.[16] First, they cite the U.S. State Department's dedication to OSAC through heavy investment in its individual success as a Federally sponsored program.[17] Provided with the necessary budget and support, OSAC has grown significantly since its original founding, with over 5,500 U.S. companies and organizations counted among its membership.[18] Alongside this, according to the authors, was the "appointment of high-level senior officials in the headquarters to oversee and iterate the partnership framework to ensure that it represented a value proposition for all involved". Indeed, in September 2021, Ellen K. Tannor, a 19-year veteran of the Diplomatic Security Service (DSS), was named OSAC's new Executive Director having previously served as the Security Advisor to the U.S. European Command (EUCOM) in Stuttgart, Germany, further demonstrating the U.S. State Department's continued commitment to encouraging high-level senior personnel to support the public-private partnership program.[19]

The second key characteristic the authors note was the creation of the International Security Foundation (ISF), through which private-sector partners now contribute their own resources to support OSAC activities directly.[20] According to its mission statement, ISF was founded in 2011 as a nonprofit, a 501(c)(3) tax-exempt educational organization, "to fund information-sharing programs and networking to enhance the support of the global security community working to keep Americans and American interests abroad safer and more secure."[21] ISF's work therefore continues to support the OSAC mission more broadly, and

helps to provide additional resources for maintaining and growing the ongoing partnership between the U.S. State Department and the private sector.

According to Concannon and Center, the third characteristic for success is OSAC's ability to adapt in order to allow the partnership between the public and private sector to develop naturally over time.[22] In this way, they continue, "flexibility is important to avoid a cookie-cutter approach that is unresponsive to partners' specific goals and needs in particular areas or sectors, and it supports the development of the most crucial aspect of any partnership—strong relationships".[23] Part of OSAC's continued success is its ongoing engagement with its private sector partners, whether through its subset of regional councils (focused on specific regions around the world), by industry working groups (i.e., Media & Entertainment, Transportation/Aviation, Finance, etc.), or through its use of technology-based information sharing. OSAC employs a number of regional analysts who provide ongoing support for the organization through research and analysis dedicated primarily to the cross functional interests of the U.S. private sector. OSAC also offers its members up to date safety and security-related information, public announcements, State Department bulletins, travel advisories, significant anniversary dates, terrorist groups profiles, country crime and safety reports, special topic reports, and foreign press reports, among many other resources. Finally, OSAC has created a network of country-specific councils around the world that brings together U.S. embassies and consulates with the local U.S. business community to share security information and best practices.

OSAC has proven to be a valuable resource not only for the U.S. government, but for American companies seeking to establish domestic and international partnerships in order to secure their business interests and protect their assets and, by extension, the assets of the United States more broadly. By examining OSAC's continued success as a public-private partnership program between the U.S. State Department and the American private sector, the Foreign Malign Influence Center (FMIC) may find a model example for its own future engagement with private sector industries.

V. Public – Private Sector Interview Results

V (a). Public Sector Responses

Just as there remain significant gaps on the private sector side, there exist a variety on the public sector side when it comes to engaging in countering disinformation and malign foreign influence. In April 2021, the Office of the Director of National Intelligence (ODNI) announced the establishment of the Foreign Malign Influence Center (FMIC), for the purpose of consolidating intelligence from across the Intelligence Community (IC) on malign foreign influence, as well as assessing and warning about foreign malign influence efforts. The center was established at the direction of Congress, which legislatively required the ODNI to establish a center to integrate intelligence from across the IC on malign influence, particularly as it related to threats from Russia, Iran, North Korea, and China.[24] Since April 2021, the ODNI has encountered a variety of challenges with regards to opening the FMIC

officially due to budgetary questions, as well as issues pertaining to the size and exact purpose of the FMIC.[25] However, this new FMIC, when officially established, could directly contribute to the effort to better integrate the public and private sector engagement on countering disinformation. As a result, our team had the opportunity to interview Dr. Jake Shapiro, a professor at Princeton University, who is presently assigned to the ODNI to assist with establishing the FMIC to discuss how the FMIC intended to bridge this gap, as well as what gaps and challenges remain.

During the interview Dr. Shapiro discussed several key matters when it comes to public – private engagement on countering disinformation including: the current status of public – private engagement; how the FMIC intends to fill existing gaps as well as enhance existing relationships; and identify remaining significant challenges in this field. As noted earlier, considering the FMIC remains in flux officially pending Congressional and ODNI considerations, but Dr. Shapiro was able to outline some positive developments when it comes to public – private partnerships on countering disinformation, as well as areas where the private sector, outside public sector engagement, could enhance its capabilities to counter disinformation.

According to Dr. Shapiro, there are presently two entities within the ODNI responsible for outreach to the private sector including the Analytic Exchange Program (AEP) and a technology engagement office, but they have specific missions outside foreign malign influence. There are entities in specific U.S. government agencies such as the Foreign Influence Task Force (FITF) at the FBI and different mission centers at the CIA that have developed positive relationships with certain companies, but there is not one overarching entity responsible for communicating with the private sector. While these relationships are significant and positive, they remain piecemeal, and the private sector has expressed an interest in developing a list of a smaller number of higher profile or responsive contacts in the U.S. government that can act as traffic cops, ensuring the appropriate, knowledgeable point of contact is connected with their private sector counterpart. However, Dr. Shapiro did emphasize that some duplication is to be expected and helpful, as one does not want just one entity and one USIC agency to be focused on foreign malign influence, as each can bring its own experience and specialty to bear when engaging with the private sector.

In addition to the relatively piecemeal nature of engagement across the USIC with members of the private sector on malign influence and disinformation, there is also the challenge of who in the private sector is actually engaging with the U.S. government. Often, it is former USIC employees who moved to the private sector, such as at Meta, and they often are not the appropriate individual to be engaging with the USIC as they may not be leaders of the investigative bureaucracy. Additionally, Dr. Shapiro noted the importance of regular engagement with representatives from the private sector, something that does not happen with consistency at this time, and something that can only happen when there is an established, senior point of contact with which to engage. Despite these challenges, Dr. Shapiro noted there were several ways the FMIC intended to bridge gaps with the private sector.

Aside from acting as a formal interlocutor between the private sector and the USIC to provide consistent messaging, the FMIC also intends to establish more traditional engagement opportunities such as conferences and teleconferences to ensure USIC members and private sector partners develop relationships and engage on these issues. Additionally, there is clear hope that the FMIC can aid private sector partners in coming together and sharing their respective resources and information when combating disinformation on their platforms. For example, Dr. Shapiro cited the example of how the U.S. nuclear power industry recognized, after the incident at Three Mile Island, the importance of all relevant parties collaborating on key safety issues and establishing an organization that focused on safety at nuclear plants with which all companies coordinated. Similarly, for example, social media companies may benefit from establishing some entity to coordinate across platforms and share what each is witnessing when it comes to disinformation, but which is aided by guidance and collaboration from the FMIC.

Despite the positive opportunities for the FMIC to insert itself into the dialogue between the private sector and the USIC, there remain significant challenges. As Dr. Shapiro noted, there is no real system in place across the social media companies to share what one another are witnessing when it comes to disinformation, and as foreign malign influence actors continue to adapt and change their messaging, this remains a huge challenge as the actors could easily jump from one platform to another as their activities are being identified and shut down. Additionally, there remains a gap in the USIC when it comes to understanding how the private sector is structured, and, on the private sector side, there is an understanding, but it is limited. This also is a significant challenge for both sides, as not knowing how your respective partner is structured and addresses challenges can mean not knowing who to reach out to in order to address an issue. As Dr. Shapiro noted, however, this remains an area the FMIC hopes to contribute to improving.

With the FMIC still in its infancy, there remain significant gaps as to how and what the FMIC will do in the long term to enhance the relationship between the public and private sectors when it comes to countering disinformation. What is clear is there are significant gaps within and between the two sectors that could benefit from an actor such as the FMIC to aid in communicating between one another, as well as to effectively mitigate the threat posed by these foreign malign influence actors.

V (b). Private Sector Responses

During the course of our research our team attempted to engage directly with a number of private sector entities, particularly in the technology sector. The topic of misinformation and disinformation can often present itself as ultra-sensitive, especially when in discussions with companies whose main products and services are connected directly or indirectly to the propagation of malign foreign influence (MFI). Still, by engaging with these companies and encouraging their participation in our anonymous survey, our team hoped to glean insights into how the FMIC may seek to establish a future public-private partnership on the issue of MFI affecting the homeland. Ultimately, we received answers from only one private sector company, though those answers did shed light on some of the areas that may be worth highlighting for future research and engagement.

The company that answered our survey described how their current interactions with the U.S. government regarding the issue of MFI are done primarily via analysts connected to the Federal Bureau of Investigation and is conducted through "semi-regular" information-sharing sessions. They note that the FBI will provide "semi-regular" reports on MFI trends impacting digital platforms more broadly but will also seek information about specific bad actors from this company's internal teams. The company also noted that they engage with several agencies from the Federal government on this topic and that their engagement is not limited to a single point of contact.

The company described its willingness to engage with any additional partners in the public sector that are interested in working with it directly to counter the issue of MFI and noted specifically that regular conference calls and/or meetings regarding MFI in their specific sector would be the most beneficial, stating "regular updates from the federal government about MFI trends and campaigns would help us to effectively assess their impact on our platform and locate any potential bad actors."

When asked about current challenges, the company noted that their platform has had two main challenges when engaging with the federal government. The first challenge, they note, is the irregularity with which their team has received detailed information about MFI which has then led to knowledge gaps between the public and private sectors. The company then suggested that "establishing more regular lines of communication would facilitate more actionable insights for both parties." The second challenge facing the company is that the information they have received in the past has been tailored more to abuse cases prevalent on other, more prevalent platforms. Any information about MFI campaigns that is specific to this company's platform would better support them in identifying bad actors responsible for specific cases.

While only one technology company was able to provide answers for our survey questions, they do offer specific insights for what may be most relevant for a future public-private partnership with the FMIC. Furthermore, the company's engagement with our research team alongside its desire to pursue such a potential partnership are encouraging

signs that may open the door to further engagement by our team with other, more prevalent technology companies that could serve as foundational partners for the FMIC in the future.

VI. Conclusions and Recommendations

Between the researched models of success for public-private partnerships and the limited responses the team received from both the public and private sectors, our team hopes to offer the Foreign Malign Influence Center unique insight to contribute to the creation of a potential roadmap for its own success in this arena. Among the most critical recommendations provided are the following:

- Direct engagement with social and digital media companies to communicate about disinformation and better ways to counter it
- Effective coordination across civil society, government, and think tanks to collect the broadest evidence of MFI taking place
- Significant government investment into the public-private partnership project
- Significant buy-in from the private sector for networking and relationship building
- Direct access to U.S. government resources such as information-sharing
- FMIC's potential role as an interlocutor between the public and private sectors on disinformation and countering malign foreign influence
- Assist in establishing training for private and public workforces to identify and counter disinformation and to increase disinformation awareness
- Identifying key points of contact for the private sector in the U.S. intelligence community for engagement and information sharing in a more structured way
- Facilitating conferences and seminars between the U.S. intelligence community and the private sector for more direct engagement on the issue of MFI
- Regulating ongoing direct communication with the private sector on rising trends and current MFI campaigns
- Enhancing information sharing with private sector entities by tailoring the relevancy of the information being provided to each company specifically

Although significant monetary and resource investment by the government is critical for the success of the public-private partnership project, enhancing information sharing with private sector entities and ensuring the relevancy of that information for each company will enable a more tailored approach to tackling the issue of MFI across a larger cross section of the private sector.

ANALYTIC DELIVERABLE DISSEMINATION PLAN

- ODNI's Foreign Malign Influence Center
- Cybersecurity and Infrastructure Security Agency
- Relevant Entities at:
    - Snap, Inc.
    - Meta (and subsidiary entities):
        - Facebook
        - WhatsApp
        - Instagram
    - Twitter
    - TikTok
    - Discord
- Microsoft

Endnotes

[1] Robbins, Joseph | Pub 23 September 2020 | "Countering Russian Disinformation" | *Center for Strategic & International Studies* | https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation | Accessed on 20 July 2022.

[2] Tsitsikashvili, Mariam | January 2020 | "Comparing Lessons Learned from Countering Russian Disinformation in Georgia and the Czech Republic" | *Kremlin Watch* | https://www.kremlinwatch.eu/userfiles/comparing-lessons-learned-from-countering-russian-disinformation-in-georgia-and-the-czech-republic.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=kremlin_watch_briefing_countering_russian_disinformation_in_georgia_and_the_czech_republic&utm_term=2020-01-17 | Accessed on 20 July 2022.

[3] Robbins, Joseph | Pub 23 September 2020 | "Countering Russian Disinformation" | *Center for Strategic & International Studies* | https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation | Accessed on 20 July 2022.

[4] Tsitsikashvili, Mariam | January 2020 | "Comparing Lessons Learned from Countering Russian Disinformation in Georgia and the Czech Republic" | *Kremlin Watch* | https://www.kremlinwatch.eu/userfiles/comparing-lessons-learned-from-countering-russian-disinformation-in-georgia-and-the-czech-republic.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=kremlin_watch_briefing_countering_russian_disinformation_in_georgia_and_the_czech_republic&utm_term=2020-01-17 | Accessed on 20 July 2022.

[5] EUvsDisinfo | 22 April 2020 | "To Challenge Russia's Ongoing Disinformation Campaigns: The Story of EUvsDisinfo" | https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-the-story-of-euvsdisinfo/ | Accessed on 19 July 2022.

[6] Ibid.

[7] European Commission | 14 June 2019 | "Report on the Implementation of the Action Plan Against Disinformation" | *European Commission High Representative of the Union for Foreign Affairs and Security Policy* | https://www.exteriores.gob.es/en/PoliticaExterior/Documents/joint_report_on_disinformation.pdf.

[8] Diallo, Kesso | 2 November 2021 | "What is Viginum? The New Agency Against Foreign Digital Interference" | *L'Eclaireur FNAC* | https://leclaireur.fnac.com/article/37709-quest-ce-que-viginum-la-nouvelle-agence-contre-les-ingerences-numeriques-etrangeres/ | Accessed on 18 July 2022.

[9] Ibid.

[10] Suliman, Adela | 6 January 2022 | "Sweden Sets Up Psychological Defense Agency to Fight Fake News, Foreign Interference" | *Washington Post* | https://www.washingtonpost.com/world/2022/01/06/sweden-fake-news-psychological-defence-agency/.

[11] Ibid.

[12] "Who We Are" | OSAC.gov | Accessed on 20 July 2022 | https://www.osac.gov/About/WhoWeAre.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Security Management by ASIS International | Pub 02-27-2021 | "Public–Private Partnership Case Study: OSAC" | Accessed on 20 July 2022 | https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2021/public-private-partnership-case-study-OSAC/.

[17] Ibid.

[18] Ibid.

[19] Security Magazine | Pub 09-27-2021 | "Ellen K. Tannor joins OSAC as Executive Director" | Accessed on 20 July 2022 | https://www.securitymagazine.com/articles/96174-ellen-k-tannor-joins-osac-as-executive-director.

[20] Security Management by ASIS International | Pub 02-27-2021 | "Public–Private Partnership Case Study: OSAC" | Accessed on 20 July 2022 | https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2021/public-private-partnership-case-study-OSAC/

[21] International Security Foundation | About | Accessed on 20 July 2022 | https://isf4osac.org/about-isf/

[22] Security Management by ASIS International | Pub 02-27-2021 | "Public–Private Partnership Case Study: OSAC" | Accessed on 20 July 2022 | https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2021/public-private-partnership-case-study-OSAC/
[23] Ibid.
[24] Matishak, Martin | 26 April 2021 | "Intelligence Community Creating Hub to Gird Against Foreign Influence" | *Politico* | https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604 | Accessed on 22 July 2022.
[25] Merchant, Nomaan | 10 January 2022 | "US Delays Intelligence Center Targeting Foreign Influence" | *Federal News Network* | https://federalnewsnetwork.com/workforce/2022/01/us-delays-intelligence-center-targeting-foreign-influence | Accessed on 22 July 2022.