THREAT ASSESSMENT

“DECLASSIFY YOUR WAY TO DETERRENCE”

A CASE STUDY OF CLASSIFIED INTELLIGENCE USED TO DETER RUSSIAN AGGRESSION, AND THE HISTORICAL USE OF SUCH METHODS

Elijah Woodward
PS636-T301: Deterring the Enemy: Case Studies in Strategic Deterrence
May 27, 2024

THREAT AND THESIS

This paper seeks to conduct an assessment on the deterrence value of the monumental amount of "deeply secret" information that was declassified and publicly shared by the United Stated Government and United States Intelligence Community in the run-up to the February 2022 Russian invasion of Ukraine. This assessment will look at the uses of declassified intelligence both in the February 2022 case and compare this against historical cases of declassified intelligence that was used for strategic deterrence aims. Finally, the advent of Artificial Intelligence entering mainstream lexicon and use has spurred questions around how Artificial Intelligence can be used to aid in deterrence and strategic deterrence. Specifically, this paper will look at the use of artificial intelligence by private sector companies in 2023 and 2024, especially with targeted ads. While this may seem initially like a disconnected and unrelated subject, this actually has a direct corollary to the end goals of deterrence: to sway or persuade a target audience to react in a desirable fashion.

INTRODUCTION

Typically, deterrence is meant to dissuade a target audience (be it a nation-state, a dictator, or a military program) from undertaking certain aggressive actions. The use of Artificial Intelligence to aid in the identification of material that can and should be declassified should be considered given the massive amount of data that is collected on a regular basis.

However, this is not the first time the use of Artificial Intelligence to aid in processing intelligence has been considered. According to a publicly released memo from the Central Intelligence Agency, the CIA hosted an Artificial Intelligence symposium in 1985 which included the use of AI to process the explosion in data intelligence agencies were collecting at

the time.[1] Although 40 years have elapsed since this conference, the same tools are being described to solve the same problems. However, the capabilities of such tools are becoming more clear today, and their ability to generate hypotheses, alternative and competing theories, and explore "brainstorming" opportunities for analysts seeking to identify methods of deterrence using declassified information offers new capabilities not previously readily obvious.

EXTENT OF THREAT TO THE US AND OTHER COUNTRIES

The use of declassified intelligence and using that in the public sphere is not a phenomenon that is restricted to just the United States. Israel has routinely declassified intelligence, as was the case during their attacks on a nuclear facility in Syria in the 2000's.[2] Russia claims to be releasing classified material in response to the "bio labs" they claim they have found that proves the United States was using Ukraine as a hub for bioweapon engineering prior to the 2022 invasion[3], and as justification for their invasion.

This has lead to the United States sharing unprecedented amounts of information as documented in a 2024 Time magazine article about this exact phenomena.[4] Western governments have, for years, had an informal system of, at times, declassifying information through "leaks" that end up in the media conveniently. Although this may not have followed traditional legal channels, without a doubt these opportunistic leaks helped shape foreign policy, shame competitors when needed, and shape and guide conversations and rhetoric where needed.

EXAMPLE: BRITAIN WEAPONIZES LEAK AGAINST THE US

---

[1] "ARTIFICIAL INTELLIGENCE SYMPOSIUM | CIA FOIA (Foia.cia.gov)." 1985. Www.cia.gov. Accessed April 5, 2024. https://www.cia.gov/readingroom/document/cia-rdp87m00539r000600730001-2.
[2] "Israel Confirms Syria Reactor Strike | Arms Control Association." n.d. Www.armscontrol.org. Accessed May 27, 2024. https://www.armscontrol.org/act/2018-04/news-briefs/israel-confirms-syria-reactor-strike.
[3] "Pentagon Divulges Number of US-Funded Biolabs in Ukraine." n.d. RT International. Accessed May 27, 2024. https://www.rt.com/news/556902-pentagon-ukraine-biolabs-wmd/.
[4] Calabresi, Massimo. February 289, 2024. "Inside the White House Program to Share America's Secrets." 2024. TIME. https://time.com/6835724/americas-intelligence-secrets/.

For example, in 2003 a British intelligence analyst named Katharine Gun leaked a request from the United States to British intelligence, asking for assistance in monitoring other countries from the Untied Nations as a result of votes regarding the United States' intent on going to war with Iraq. As history has taught us, the American campaign was globally scorned, and this raises the possibility that the leak of this request to British Intelligence could have been an orchestrated method of statecraft to manipulate the United States and put a check on behavior that the British may have determined was violating acceptable behavior in international norms. It is also worth noting that the analyst was never charged for her role in the leak, which is incredible given the sensitivity of the information and clear violation of the Official Secrets Act. The decision to not charge the analyst was publicly stated as "not enough evidence" despite public acknowledgements at the time by the accused herself.[5] The analyst has gone on to have a career and live a free life, even having books and a movie made about her actions.

If this truly was a case of an ally using classified intelligence and intelligence requests and deterring the United States by publicizing this through unorthodox methods, this could truly be a case of a dual-use weapon that has been used by the United States and has also been against the United Stated by her own allies.

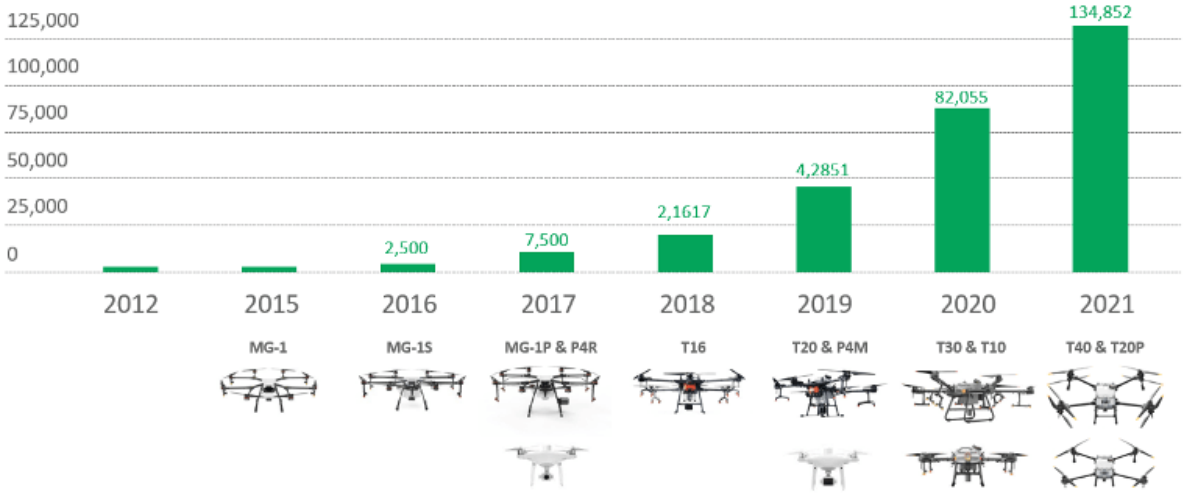
SOCIO-ECONOMIC CONSEQUENCES

The impacts of declassified intelligence can potentially have knock-on effects and second order ramifications, and not stay limited directly on the subject matter itself. For example, in 2017 it was revealed in a "leaked" memo from the Department of Homeland Security that DJI drones were suspected of sending data back to China based on patterns of land purchases that had been observed in Northern California after DJI drones had been used for agricultural

[5] Frankel, Glenn. February 25, 2004. Washington Post. 2024. "British Whistle-Blower Avoids Charges," January 26, 2024. https://www.washingtonpost.com/archive/politics/2004/02/26/british-whistle-blower-avoids-charges/5cf2a940-3a29-43ca-b803-545df1964889/.

purposes.[6] The obvious implications almost immediately in this case is the potential for sales of DJI drones to be impacted and cause economic consequences to the companies that may be operating these drones and offering services, even if the companies themselves have no connections to the Chinese government and in fact may be truly oblivious themselves to the risks posed by these technologies.

This, again, also had the potential of deterring continued data acquisition by the Chinese government and to spell out potential consequences and deter future data collection. However, according to data released by the DJI manufacturing company themselves, it seems these revelations had little if any impact on sales, and according to DJI Agricultural statistics, the use of DJI agricultural drone use grew from 2,500 in 2016 to over 130,000 five years later in 2021.[7]



THEORIES

[6] Mozur, Paul. 2017. "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say." The New York Times, November 29, 2017, sec. Technology. https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html.

[7] "DJI Agriculture Released the Agricultural Drone Industry Insights Report (2021), Exploring Best Practices for Agricultural Drones - DJI." n.d. DJI Official. https://www.dji.com/newsroom/news/agricultural-drone-industry-insights-report-2021.

The Centre for International Governance Innovation (CIGI) is an independent think tank that produces peer-reviewed research and independent analysis. In a 2022 article published by the CIGI, the strategic leaking of intelligence and the strategic declassification for deterrence aims, specifically against Russian aggression late 2021 and into 2022, was examined. As Carvin notes, "In addition, these activities involve a clear blurring of intelligence with information operations. Of course, all information operations are based on some kind of intelligence — but in this case intelligence is the operation itself, not merely what underpins it."[8]

Just Security is a forum focused on the rigorous debate of security topics, and in March 2024 published an analysis of comments recently made by Director of National Intelligence Avril Haines on the issue of disclosing secrets and how this new policy of transparency could be shaped. Part of the problem cited by Rosen is the issue of trust, which the United States is still attempting to rebuild after the 2003 Iraq invasion and the supposed disclosure of weapons of mass destruction.[9] The use of declassified, or leaked, intelligence now runs the risk of politicization and could adversely impact the deterrence aims. If the intelligence disclosure is being done to seek political points or score wins, the deterrence aspect may be diminished if opposing threat actors can merely dismiss the disclosures as political gerrymandering and games from those seeking to deter threats.

ASSESSMENT OF STRENGTHS AND WEAKNESSES

The criticism that the Intelligence Community has a long way to go to rebuild trust through these transparency efforts is very valid. The problem of leaks being used for politically motivated purposes goes back decades. This presents an inherently problematic position for

[8] Carvin, Stephanie. 2022. "Deterrence, Disruption and Declassification: Intelligence in the Ukraine Conflict." Centre for International Governance Innovation, May 2, 2022. https://www.cigionline.org/articles/deterrence-disruption-and-declassification-intelligence-in-the-ukraine-conflict/.
[9] Rosen, Brianna. 2024. "Disclosing Secrets: Deterrence, Diplomacy, and Debate - Reflections on Remarks by DNI Avril Haines." Just Security. March 1, 2024. https://www.justsecurity.org/92934/disclosing-secrets/.

intelligence professionals attempting to use this method for deterrence: it can potentially be dismissed by the opposition as politically motivated and lacking actual substance. Trust can be enhanced if leaks against political opponents are stopped. Leaks from the intelligence community have been such a critical issue for several decade that the CIA explored the creation of a database to track all leaks in the media to identify common trends and root out the leaks in 1983.[10] This came after previous research of a large number of leaks from intelligence community that lead to requests for analysis of the leaks in 1971.[11]

As far as strengths for this new theory of deterrence, which I will name "Declassification Deterrence Theory," I believe this has real potential and has likely already saved lives. The use of this practice may not have prevented the Russian invasion of Ukraine in 2022, but so far massive use of weapons of mass destruction have not been observed in Ukraine, despite clear and specific warnings from the White House of ways they believed Putin was about to use them. This could be seen as evidence of this policy working and having a very real deterrence effect in our modern world.

CURRENT POLICY

The United States' current policy on the use of declassified information seems to, at least currently, be in a state of significant overhaul and revamping. Since before the invasion of Ukraine in 2022, the Biden White House has been consistently declassifying significant amounts of classified intelligence in an effort to highlight the behavior of Russian aggression, deter potential false flag operations, dispel lies, and do disinformation control before it can even get out of the gate and have a life of its own. This has been followed by a wide range of articles

[10] "INTELLIGENCE LEAKS | CIA FOIA (Foia.cia.gov)." November 3, 1971. Www.cia.gov. Accessed April 7, 2024. https://www.cia.gov/readingroom/document/cia-rdp83b00823r000100100007-9.
[11] "INITIATIVES to DEAL with LEAKS | CIA FOIA (Foia.cia.gov)." January 10, 1982. Www.cia.gov. Accessed April 7, 2024. https://www.cia.gov/readingroom/document/cia-rdp94b00280r001200030003-0.

published in magazines like Time which featured an in-depth interview with a variety of key intelligence figures in the White House discussing the current policy of declassifying information to deter aggression, stating, “But the world of secrets is changing, and America is scrambling to adapt.” (Calabresi, 2024) The interview with National Security Adviser Jake Sullivan highlights that the US recognizes it needs to adopt new practices and change to adapt to the new world, and fight three problems at once: disinformation, overclassification, and public distrust. (Calabresi, 2024) Sullivan recognized that we are in a “crisis of trust” and believes that such strategic transparency can have long-term, deep impacts through sharing tactical information in the here and now.

The origins of this current course of action appear to be following in the footsteps of recommendations laid out in 2021 from Chatham House. A policy paper from Kier Giles noted a number of policy recommendations, most relevant here was “Naming and Shaming.”[12] Giles stated:

> Despite apparent reluctance on the part of US and allied armed services to detail the level and potential dangers of Russian activity run against them, this paper and others have described precedents showing the clear benefits of transparency. Concealing the true nature, volume and intent of Russia’s irresponsible behaviour cedes the information space to Moscow instead of properly educating Western publics about the brinkmanship practised by Russia and the restraint required from NATO partners. In particular, it allows Russia to further the narrative that it is behaving responsibly and that NATO is the provocative actor. (Giles, 2021)

[12] Giles, Keir. "Outlook and Policy Recommendations." In What Deters Russia?, Chatham House – International Affairs Think Tank, September 23, 2021. Accessed May 25, 2024. https://www.chathamhouse.org/2021/09/what-deters-russia/04-outlook-and-policy-recommendations.

Whatever reluctance the United States and allies may have been demonstrating in 2021 seems to have evaporated since this was published. It seems the US and western allies have leaned in heavily to this recommendation in an effort to retake the narrative from the Kremlin.

The Centre for International Governance Innovation recently discussed this new policy and stated, "…deterrence and disruption through declassification are being heralded as twenty-first-century weapons…" (Carvin, 2022) highlighting the impact of the declassified intelligence in the modern era.

The Director of the Central Intelligence Agency, William Burns, took to Foreign Policy magazine in 2024 to also highlight the American shift in the use of classified information, referring to it as "strategic declassification," and defining it as, "the intentional public disclosure of certain secrets to undercut rivals and rally allies."[13] This again is done in an effort to thwart Russian aggression, however Burns also goes on to discuss the challenges of the current time and addresses problems involving China and Xi Jinping's focus on Taiwan.

The current policy appears to be that of "strategic transparency" and is still in the process of being formalized and tuned to more appropriately meet the problems of the modern era. This coincides with the post-COVID era of Chinese-US relations hitting a stark low, the Russian invasion of Ukraine followed by the massive international response including severing various ties and mounting sanctions, and the ongoing cyber attacks we see each country conducting against each other. This heavily contested environment and era has resulted in the White House and western governments leaning more on intelligence to disclose tactical activity from classified sources in order to gain trust and dissuade actors from taking particular actions – a form of deterrence. However, this is a bit different from years prior.

[13] Burns, William J. 2024. "Spycraft and Statecraft." Foreign Affairs. January 30, 2024. https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns. https://archive.is/Gmuzh

METHODOLOGY

The majority of the research on this area is focused on case studies and qualitative research. Due to the inherently complicated and opaque nature of statecraft, intelligence tradecraft, and proving what never happened, quantitative/survey based research is exceedingly difficult in this particular subject matter.

ACADEMIC THEORIES AND DISCUSSION

The use of classified information over the years to sway public opinion or reduce the risk from threatening actors has a legacy dating back at least 60 years to the Cuban Missile Crisis of the 1962 and the Iraq "Weapons of Mass Destruction" debate from the early 2000's. These examples have provided stark contrast to each other, but in some ways lay the groundwork for the information operations (IO) we see happening today and the use of declassified information to support such information operations.

Of course, when speaking about the history of information operations, we can not neglect the role of the Gerasimov Doctrine, published in 2013 by Russian General Valeriy Gerasimov. Gerasimov's idea on "Hybrid Warfare"[14] has been oft-discussed, and is seen as the new frontier in Russia-NATO confrontations. Arcos, et all, points out that the very existence of the Gerasimov Doctrine and ideas for Hybrid Warfare, now over a decade old, could be evidence of traditional NATO deterrence methods being effective, causing Russian hybrid warfare to become the default method due to the lack of traditional means of confrontation.

The echoes of Iraq 2003 still haunt the minds of analysts and policymakers, and the disclosure of classified information to shape public opinion and justify use of force has left some leery. Many could not believe the warnings about incoming largescale land warfare in Europe, in

[14] Arcos, Rubén, Irena Chiru, and Cristina Ivan, eds. Routledge Handbook of Disinformation and National Security. Routledge, 2023.

2022, citing the leadup to the Iraq war, “Many others no doubt, remembered the warnings of ‘intelligence’ on Iraqi weapons of mass destruction in 2002 and 2003 and assumed that this was another example of ambiguous Western intelligence being spun and broadcast for political ends.”

History also leads to one of the highlights of the risks of using classified intelligence in that it could actually halt adversary behavior, creating a two-edged sword where the adversary changes course leaving the warnings left looking inaccurate. “There is also the risk of the self-negating prophecy. By using intelligence of an impending attack as part of a deterrence posture, states may negate the very thing they assess as likely, thus rendering their assessment apparently wrong. This occurred in the 1961 Iraq Kuwait crisis.” (Dylan, et all, 2022) While this particular example does not rely solely on the use of declassified information, it does highlight one of the risks policymakers are no doubt aware of and keen to avoid: classified information becoming the “self-negating prophecy.”

Reflecting back on recent history, this sort of prophetic hit and miss has been seen in the recent Ukraine conflict. As Schiffner notes:

> In the weeks and months following its deterrent threat, the United States declassified and shared intelligence with allies and partners. The U.S. disclosed Russian troop movements, attributed false-flag attacks to Russian operatives, and refuted Russian reports of Ukrainian attacks and atrocities. By undermining Russia's disinformation campaign, the United States deprived Russia of key victories in the information domain, making it more challenging to achieve its military objectives and contributing to a strategy of deterrence through denial. As support for the U.S. position grew, additional

leaders from various nations threatened Russia with economic sanctions, military build-ups, and energy boycotts while promising aid and support for Ukraine.[15]

Here we see that the disclosure of certain claims by Russia, while they did not always prevent the Russian propaganda machine from attempting to use those particular gambits, probably did a significant amount of damage to the effectiveness of those tactics and helped rally allies to the cause of Ukraine, helping the speed of response become that much more effective and immediate and making the sting of Putin's actions felt more acutely.

FINDINGS

The effectiveness of such a policy is certainly still up for debate. When we look at the question of Ukraine, we must certainly evaluate – did it prevent Moscow from invading? And the answer is very clearly and obviously, no, it did not. However, when we look at some of the specific warnings around use of WMD's and other war crimes the Russians may have been willing to commit themselves and then cast blame on to the Ukrainians, this may have indeed prevented the use of certain biological or other agents. This has not stopped Russia from using the "Biolabs" conspiracy theory, claiming that Kyiv has become an epicenter of bioweapon development conducted in partnership with the United States Government.

This creates an inherently complex and difficult question to answer, that has been wrestled with by governments alike over the ages: how do you prove (and take credit) for what you prevented from happening?

Another matter of effectiveness is the demonstration of capability. Some argue that the use of declassification is not just to prevent certain actions from being taken, but also to highlight the capabilities. When referring to deterring China in space, one source noted that, "General

[15] Schiffner, Ryan. September 5, 2023. "Declassified Intelligence and its Ability to Strengthen Coercive Threats." Naval War College. https://apps.dtic.mil/sti/trecms/pdf/AD1211088.pdf

Hyten asserted that the goal of this declassification was to 'send a message to the world that says: Anything you do in the geosynchronous orbit we will know about. Anything.'"[16]

And certainly declassified operations can have deterrence effects in more than one domain as well. While much of the recent and newsworthy examples that get attention focus on the physical and possible WMD weapons concerns in Ukraine, the cyber domain has also seen a significant amount of "signaling" so to speak using this method. Offensive cyber operations have been used more robustly in recent periods as a way to stop aggressive cyber activity, or shut it down preemptively. For example, leading up to recent elections, the TrickBot malware infrastructure was specifically targeted and their operations stymied in an effort to safeguard the election. This action was subsequently discussed in the open media, though there was no formal press conference declaring it, the classified operation was revealed. As Tate and Bates point out:

> Persistent, public disclosure is necessary for offensive cyberspace operations to deter malicious cyber activities, nested with US strategic guidance, and achievable based on recent cyberspace operations. The concept of transparent offensive cyber persistence combines cyber persistent engagement with calculated, post factum disclosure of operations information to influence the cost-benefit decisions of malicious cyber actors. This will shape international behavior by deterring the scope and aggressiveness of malicious cyber activities and encouraging like-minded allies to act in kind.[17]

Yet again, it is difficult to say exactly what activity was stopped when it never happened, and the general public was never aware of what the threat was that triggered the actions to shut this down. However, perhaps that is because the operations are not meant for the general public

---

[16] Langeland, Krista, and Derek Grossman. Tailoring Deterrence for China in Space. Rand corporation, 2021.
[17] Tate, Ryan, and Chad Bates. "Deterrence Thru Transparent Offensive Cyber Persistence." The Cyber Defense Review 7, no. 4 (2022): 227-246.

in this case: they are meant for the adversaries and to send a warning, and deter future operations.

APPLICATION

In researching this topic, it has highlighted the ways statecraft and intelligence tradecraft can work together, to both shape international norms, and also moderate behavior. By calling out bad behavior preemptively it seems it is plausible that one can use the power of intelligence, and the entirety of the intelligence community, to create a balancing effect against the hybrid warfare Russia has been waging against the west for the last 10 years. This hybrid warfare has been exceedingly difficult for the United States to counter, and it is certainly fair to say that Moscow has taken the lead in the information space.

Understanding the intricacies of the dance between both the intelligence community, the State Department, and how they interplay with foreign policy is a complicated tapestry with many threads weaving through it. This has also highlighted the difficulty in responding to the new "grey zone" of warfare, or hybrid warfare. As some have noted, "…hybrid warfare is old wine in new bottles. Nevertheless, it remains a good wine well worth drinking."[18] While this is a valid point, figuring out the new way to combat this "old wine" may lead to some discomfort in sharing intelligence previous retained. However, there do appear to be some positive results.

POLICY

In the short-term, this policy appears to be gaining significant support from allies and domestic audiences. As mentioned elsewhere, the intelligence community is likely benefiting from the "rehabilitation" of its reputation which has seen one body blow after another to tarnish its reputation and image. The failures of 9/11 were followed by the "WMD" fiasco of Iraq, which

[18] Weissmann, Mikael. "Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework." Journal on Baltic Security 5, no. 1 (2019): 17-26.

lead to a series of high profile leaks and spying scandals with Chelsea Manning and Edward Snowden revealing constitutional quagmires of spying and broken trust in the IC. While oversight is a core part of the intelligence community today, and continues to be, this paper does not seek to establish to the reader that the IC has a reputation problem

Hopefully this rehabilitation can lead to a long-term rebuilding of trust with the IC and the public, as well as with lawmakers and policymakers. This can also create the opportunity for new statecraft, new problem-solving, and new innovation across all of these fronts. As already mentioned, declassified satellite images turned out to be a windfall for archeologists – the overlapping interests of other groups with yet to be discovered interests in declassified intelligence are likely to present new opportunity for evolution, and revolution, in the terms of innovation and creative problem solving.

At the same time, the concerns about disclosure of sensitive sources and methods is not one to take lightly. While one disclosure itself may not be enough to signal to an adversary where they are vulnerable, enough disclosures could provide enough data for the adversary to begin quantitatively examining the issue and taking steps to align their security posture and close off the "access" that was providing the intelligence. This can be costly, both in terms of dollars and knowledge/intelligence lost, not to mention the potential human cost.

CONCLUSION

One of the most profound issues that still haunts the Intelligence Community is the incredible amount of data to process and determine what is actionable, and further distill what is eligible for declassification. This sort of activity is strenuous, and sifting through large amounts of data to encourage better results has been specialty of social media companies for almost two decades now. Recent reports indicate Meta (Facebook) has been using artificial intelligence to develop better advertisement campaigns and targeting, noting that the use of AI has lead to a 7%

increase in engagement.[19] This also works by using AI to identify which target markets and audiences are most likely to engage with the advertisement and delivering it where it will have the most effectiveness.

The goal of strategic declassification and "declassification deterrence" is to have an effect and impact on behavior. Whether it is changing a course of action to better align with the good of the global community or sway an unconvinced public, it is important to realize that declassification deterrence is an advertising campaign, and therefore, information operations. Very similar to advertising, these disciplines have profound overlap and could benefit from using the same tools to help solve problems in the other's domain.

[19] Hutchinson, Andrew. Feb 8, 2024. "Meta Shares Notes on the Development of Its AI-Based Ad Targeting Systems." n.d. Social Media Today. Accessed May 5, 2024. https://www.socialmediatoday.com/news/meta-shares-notes-development-ai-based-ad-targeting-systems/707069/.

Bibliography

Arcos, Rubén, Irena Chiru, and Cristina Ivan, eds. Routledge Handbook of Disinformation and National Security. Routledge, 2023.

"ARTIFICIAL INTELLIGENCE SYMPOSIUM | CIA FOIA (Foia.cia.gov)." 1985. Www.cia.gov. Accessed April 5, 2024. https://www.cia.gov/readingroom/document/cia-rdp87m00539r000600730001-2.

Burns, William J. 2024. "Spycraft and Statecraft." Foreign Affairs. January 30, 2024. https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns. https://archive.is/Gmuzh

Calabresi, Massimo. February 289, 2024. "Inside the White House Program to Share America's Secrets." 2024. TIME. https://time.com/6835724/americas-intelligence-secrets/.

Carvin, Stephanie. 2022. "Deterrence, Disruption and Declassification: Intelligence in the Ukraine Conflict." Centre for International Governance Innovation, May 2, 2022. https://www.cigionline.org/articles/deterrence-disruption-and-declassification-intelligence-in-the-ukraine-conflict/.

"DJI Agriculture Released the Agricultural Drone Industry Insights Report (2021), Exploring Best Practices for Agricultural Drones - DJI." n.d. DJI Official. https://www.dji.com/newsroom/news/agricultural-drone-industry-insights-report-2021.

Dylan, Huw, and T. Maguire. "The Ukraine War: A public crucible for secret intelligence." Survival 64, no. 5 (2022): 33-74.

Frankel, Glenn. February 25, 2004. Washington Post. 2024. "British Whistle-Blower Avoids Charges," January 26, 2024. https://www.washingtonpost.com/archive/politics/2004/02/26/british-whistle-blower-avoids-charges/5cf2a940-3a29-43ca-b803-545df1964889/.

Giles, Keir. "Outlook and Policy Recommendations." In What Deters Russia?, Chatham House – International Affairs Think Tank, September 23, 2021. Accessed May 25, 2024.

https://www.chathamhouse.org/2021/09/what-deters-russia/04-outlook-and-policy-recommendations.

Hutchinson, Andrew. Feb 8, 2024. “Meta Shares Notes on the Development of Its AI-Based Ad Targeting Systems.” n.d. Social Media Today. Accessed May 5, 2024. https://www.socialmediatoday.com/news/meta-shares-notes-development-ai-based-ad-targeting-systems/707069/.

“INTELLIGENCE LEAKS | CIA FOIA (Foia.cia.gov).” November 3, 1971. Www.cia.gov. Accessed April 7, 2024. https://www.cia.gov/readingroom/document/cia-rdp83b00823r000100100007-9.

“INITIATIVES to DEAL with LEAKS | CIA FOIA (Foia.cia.gov).” January 10, 1983. Www.cia.gov. Accessed April 7, 2024. https://www.cia.gov/readingroom/document/cia-rdp94b00280r001200030003-0.

“Israel Confirms Syria Reactor Strike | Arms Control Association.” n.d. Www.armscontrol.org. Accessed May 27, 2024. https://www.armscontrol.org/act/2018-04/news-briefs/israel-confirms-syria-reactor-strike.

Langeland, Krista, and Derek Grossman. Tailoring Deterrence for China in Space. Rand corporation, 2021.

Mozur, Paul. 2017. “Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say.” The New York Times, November 29, 2017, sec. Technology. https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html.

“Pentagon Divulges Number of US-Funded Biolabs in Ukraine.” n.d. RT International. Accessed May 27, 2024. https://www.rt.com/news/556902-pentagon-ukraine-biolabs-wmd/.

Rosen, Brianna. 2024. “Disclosing Secrets: Deterrence, Diplomacy, and Debate - Reflections on Remarks by DNI Avril Haines.” Just Security. March 1, 2024. https://www.justsecurity.org/92934/disclosing-secrets/.

Schiffner, Ryan. September 5, 2023. "Declassified Intelligence and its Ability to Strengthen Coercive Threats." Naval War College. https://apps.dtic.mil/sti/trecms/pdf/AD1211088.pdf

Strobel, Warren P. n.d. “Release of Ukraine Intelligence Represents New Front in U.S. Information War with Russia.” WSJ. Accessed April 7, 2024. https://www.wsj.com/amp/articles/release-of-secrets-represents-new-front-in-u-s-information-war-with-russia-11649070001. https://archive.is/4inVa

Tate, Ryan, and Chad Bates. "Deterrence Thru Transparent Offensive Cyber Persistence." The Cyber Defense Review 7, no. 4 (2022): 227-246.

Ur, Jason. "Spying on the past: Declassified intelligence satellite photographs and near eastern landscapes." Near Eastern Archaeology 76, no. 1 (2013): 28-36.

Weissmann, Mikael. "Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework." Journal on Baltic Security 5, no. 1 (2019): 17-26.