DIGITAL ASSAULT ON THE US DEFENSE INDUSTRIAL BASE

HOW US DEFENSE CONTRACTORS ARE TARGETED BY INFORMATION OPERATIONS

An Omelas Publication

INTRODUCTION

Great power competition of the 21st century differs from competition of the past, with non-kinetic capabilities having a distinct advantage in new domains. US adversaries like China and Russia are well aware of this trend and have emphasized a non-kinetic offensive arsenal. The information environment is the modern battleground of ideas and beliefs. The novel development today is the expansion of justifiable targets for offensive information warfare. Like strategic bombing campaigns of the mid-20th century, information warfare has no boundaries and an increasing proportion of society is being assailed by malicious information operations (IO).

At Omelas, we aim to shed light on how political actors, state and nonstate, are conducting influence operations online to those ends. While many of our partners have focused on the important task of exposing covert actions online, overt accounts and channels–those that make no secret of their ownership–hold positions of soaring influence and power online, often commanding the top spots among news channels or content creators of any kind. They work in tandem with internal entities and external actors to then distribute this content through both overt and covert means, including but not limited to botnets, sock-puppets, and more.

The US is a locus for information operations and the defense industrial base is a high value target for US strategic competitors who know it as the source of American military power. It is vital that we maintain the security of the defense industrial base, comprised of both large primary contractors and their subcontractors. For contractors, the concern is digital brand risk. For the US Government, the objective is to maintain the public's trust in these companies. A series of crashes involving Boeing's 737 Max serves a prime example of how consumer trust can quickly sour and affect the entire aviation industry. Most discussions about protecting the defense industrial base focus on the physical supply chain, but the social supply chain is an equally important vulnerability.

The social supply chain is an intangible structure measured in terms of public support and perceptions, directly influenced by digital media, and indirectly empowered--or compromised--by the dominant actor in the online information environment. Without positively engaged social support, the defense industrial base risks negative sentiment impacting the base's ability to effectively provide for national security.

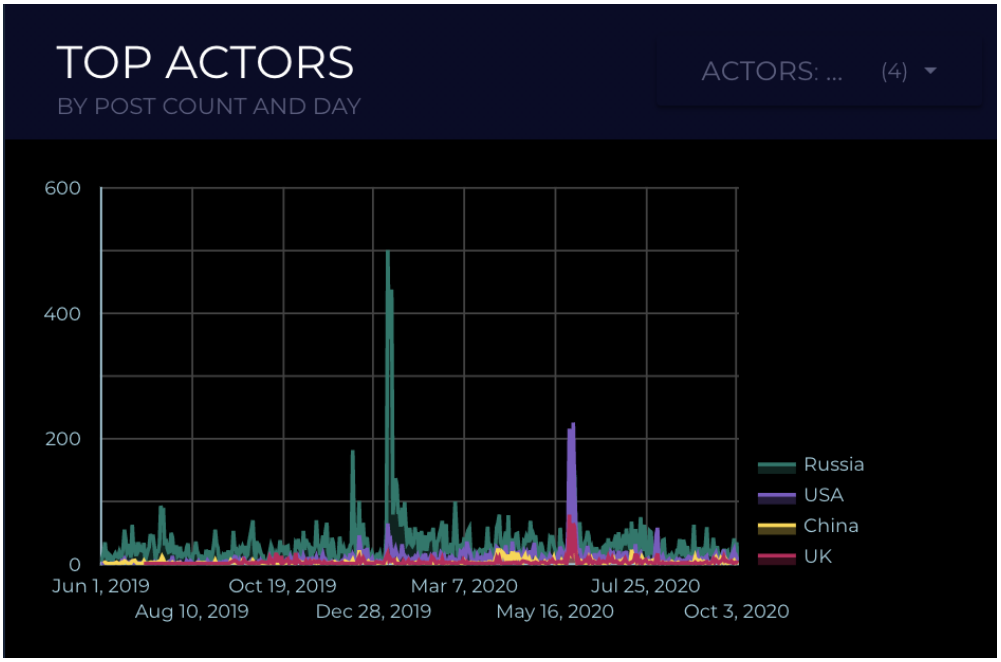
ACTORS

RUSSIA

Russia is far and away the most prolific actor in the information environment today. Accounting for more than a quarter of all content across the 200+ actors tracked in our database, Russia has an outsized and influential role in digital media. Even in content discussing US defense contractors, Russia sets itself apart as the dominant actor. Attacking defense contractors non-kinetically in the information space provides Russia with the ability to damage the industrial base underpinning American military influence.

In the last 16 months, we identified 15,839 publications coming from state-owned Russian media outlets that referenced US defense contractors or their military and commercial systems. This content is overwhelmingly negative, often focusing on the shortcomings and failures of the contractor's systems. Analysis of the content reveals a sophisticated and subtle initiative to control the narrative around US defense contractors in the global media.

Russia's strategic goal, like many of its information operations, aims to foment negative perceptions of US defense contractors, discredit them as reputable institutions, and instigate hostility among the public. The following section measures the effectiveness of Russia's approach by comparing its IO cases to other actors.



Top Actors by Post Count of Content Discussing US Defense Contractors

CHINA

China is a relative newcomer to internationally focused information operations but has constructed an impressive media presence in a short amount of time. In discussions on US defense contractors, state-owned Chinese media published 922 posts between June 2019 and October 2020. The qualitative content trends make China a compelling actor. Early on, Chinese military leadership understood the value of non-kinetic warfare and in 1999, two colonels from the People's Liberation Army wrote a military strategy manual titled 超限战, or "Unrestricted Warfare". Besides economic and international levers of influence, information warfare figures prominently as a tool to overcome the military dominance of an adversary like the United States.

China's IO approach to the US defense industry reflects much of the same strategic goals as Russia: to discredit defense contractors and to deflate public support. China recently deployed a messaging campaign in response to weapons sales to Taiwan, a long-running client of US defense contractors. This approach to IO against defense contractors suggests a defensive and reactive utilization of online messaging to retaliate against unfavorable US policies. Historically, China has threatened to sanction companies that sell weapons to Taiwan, but only recently followed through with announced plans to sanction the personnel of Lockheed Martin. Like Russian content, Chinese content is frequently focused outward to international audiences as well as internally for their domestic population. Natural language processing and analysis reveals over 50% of Chinese content appeared in English and 26% in Chinese between June 2019 and October 2020. This corresponds to past IO conducted by China, particularly their early COVID-19 narratives in which the Chinese Communist Party (CCP) sought to assuage domestic concerns and bolster support. China is an adept actor in the information environment, previously demonstrating proficient use of the TTPs covered in this report, though only a few are covered in the context of messaging on US defense contractors.

UNITED STATES

The US possesses a diverse and expansive online presence led by government accounts that promote pro-US information online. In many instances, however, US government accounts lag behind Russia and China when responding to a global event in the information environment. This approach often cedes first-mover advantages to adversaries, but in some cases the US has mounted extremely effective counter-messaging campaigns to offset adversarial narratives.

Within the context of US defense contractors, US IO demonstrates effective messaging in the long term, deflecting Russian and Chinese messaging efforts and promoting a positive image of the companies. The US government published 3,716 posts from June 2019 to October 2020 in which American defense contractors are referenced. Though far less prolific than Russian accounts, American accounts showed an impressive level of precision and impact.

The US Government's strategic goal in this context is to protect and insulate its chief providers of military equipment from negative media coverage. Moreover, the US seeks to promote the effectiveness of its contractors' systems, both as a

power signaling mechanism to adversaries and as a positive public support generator. This task is accomplished by government social media accounts belonging to the US military services, State Department, and individual foreign missions among others.

While Russia, China, and the US make up 89% of IO content referencing the defense industrial base, emergent actors like Turkey and Qatar are prolific in the information environment. Turkey published more than 400 posts with a strong negative tilt, particularly related to the US' threat to exclude Turkey from the F-35 program. Qatar also posted more than 400 times and the bulk of its content has been received positively by audiences.

TACTICS, TECHNIQUES, AND PROCEDURES

The TTPs employed by the previously discussed actors are as diverse as their overall strategic goals. Each actor's strategic focus is complemented by TTPs that enable greater audience engagement and communicate a clear message. Among the TTPs used, we focus on the "4D" model pioneered by Atlantic Council's Digital Forensic Lab (DFR), Burst Narratives, Cyber-enabled information operations, and Agenda Setting campaigns.

Cases examined here refer to multiple capabilities Omelas employs to understand and organize phenomena observed in the online information environment. To enhance the rigor of research, Omelas conducts sentiment analysis on both actors and audiences by examining content and engagements, respectively. On a scale of -1.0 to +1.0, content is graded according to how positive or negative it is, or whether actor portrayals are positive or negative.

THE 4D MODEL

The 4D model of disinformation TTPs refers to the multifaceted approach used by actors to distort, distract, dismiss, and create dismay around a given event. These techniques can be employed independently or in combination if one proves to be less effective than another. Similarly, they can be used in conjunction with other TTPs, such as burst narratives to amplify messaging and reach more audience members in a short amount of time.

In a recent case of distortion and distraction, we detected malign IO narratives against SpaceX in April 2020, ahead of its major Falcon launch. Russia was the lead actor by post count, with the headline on state-owned tabloid RT: "SpaceX Starship SN3 prototype rocket CRUMPLES like a tin can as it fails the latest test," with a video of the explosion. Two months later, after the successful launch of Space X's Falcon, Russian content pivoted the narrative to comparing the space suit worn by SpaceX astronauts to those of Russia's

Russian post suggesting SpaceX took idea for Dragon spacecraft from Russia

Falcon on the 1970s Soyuz lunar mission on TV Zvezda, an outlet owned by the Russian Ministry of Defense. Prior to SpaceX's historic May 30 launch--in which the first American astronauts launched from US soil into low Earth orbit since 2011--Russian messaging on the company is noticeably negative, scoring -0.1 on a -1.0 to +1.0 scale. Disparaging posts like above are common, but this trend completely changed to a more positive narrative following the successful May 30 shuttle launch. Russia content immediately adjusted to score +0.14 in actor sentiment and +0.11 in audience resonance.

Official accounts like Russia's Ministry of Defense carry more weight on topics of defense and national security than bots or sock puppets, making them more effective at some TTPs like distortion and dismissal. Established media outlets such as TV Zvezda carry weight in the information environment because reporters tend to trust official accounts' press releases and stories. Regardless of whether the organization is publicly acknowledged to be state-funded, reporters utilize their articles as sources even if the source material is heavily manipulated or distorted. Once information is in Western mainstream media and gains traction online, they are seen as the truth. In this respect, first-mover advantages accrue to the actor that posts first, and they can be extremely lucrative due to the vacuum of coverage when a story is actively developing. This is typical TTP out of the Russian playbook, which is also increasingly being used by other malign actors.

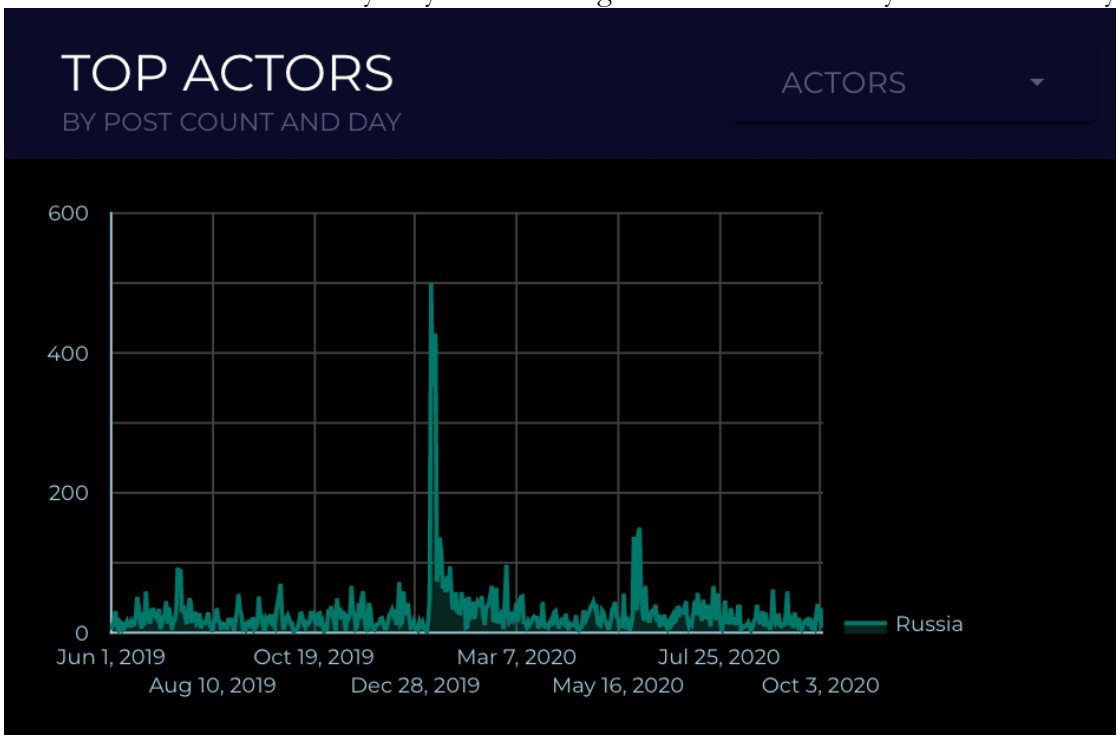
BURST NARRATIVES

Burst Narratives are an IO tactic in which an actor dramatically increases the number and frequency

of posts on a given topic. For each actor, the threshold for identifying a burst narrative is different and corresponds to the average number of posts preceding and following the spike observed. The standard applied to Russian burst narrative differs from the standard applied to China because neither actor consistently engages the online media environment the same way. Russia and China are the most prolific users of burst narratives when an important event occurs, and they employ the tactic to gain first-mover advantages in the information environment before other actors can respond.

In early January, Russia deployed the most aggressive burst narrative seen to date on the downing of Ukraine International Airlines Flight 752, first supporting Iran's early response to accusations and criticizing Boeing and the US. Between January 8th-12th, Russia posted about the downing more than 400 times every day and continued posting more than 100 times a day until January 18th. While half of this content was posted in Russian, the other half consisted of multiple foreign languages, mainly English, Arabic, Spanish, and French. This content registered a significantly negative sentiment score of -0.66 on a scale from -1.0 to +1.0. What differentiates this burst narrative from a Russian IO *campaign* is its short lifespan and messaging transience. A campaign lasts much longer than a few weeks, has a consistent narrative that connects to the actor's long-term geopolitical goals, and is proactive in messaging as opposed to reactive to an event.

Russia's narrative on the downed Boeing 737 was volatile, they initially casted doubts surrounding the circumstances of the plane crash, but then pivoted and criticized the US more broadly. This is a typical example of dismissal and distortion used in combination with a burst narrative to quickly gain control of the story. In the first 5 days



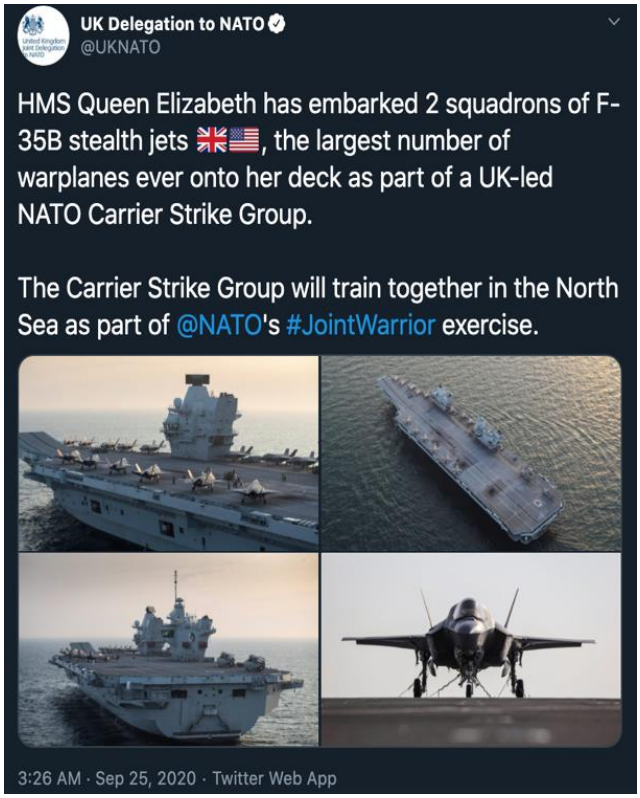
Russian Posts Referencing Us Defense Contractors from June 2019 - October 2020. Ukrainian Plane Crash Burst Narrative Occurring January 8-18, 2020

following the crash, Russia claimed the disaster was caused by a technical malfunction in the 737, and dismissed other voices that argued Tehran may have shot it down. Russia followed up saying Western intelligence services supported this conclusion, and distorted a Reuters article on the plane crash. However, Iran later admitted its military had shot down the plane and undermined Russia's narrative, whereupon Russian content stopped alluding to Boeing's culpability in the plane crash. In this case, the combined pressure of international reporting surfaced a mainstream narrative closer to reality, ultimately overcoming Russia's attempt to co-opt the narrative and shift blame.

In another recent case, China deployed a small burst narrative in response to weapon sales by Lockheed Martin to Taiwan. Between July 14-18, China made multiple posts on the CCP's announcement to sanction Lockheed following US approval of sales of Patriot missiles to Taiwan. About 25% of the content was posted in Chinese, 40% in English, and 10% in both Spanish and French. The focus on foreign languages suggests an international demographic as the audience, and an intent to demonstrate the US' role in instigating tensions between Taiwan and the mainland. The actor sentiment was relatively neutral, registering only -0.01

CYBER-ENABLED IO

Cyber-enabled IO is risky and therefore less prolific given the tactic's capacity for damage--and blowback--when conducted properly. To date, there is no evidence of a cyber-enabled IO against a US defense contractor, but the TTP's increasing prevalence reflects a serious threat. Defense contractors are a prime target for such operations given their role as providers for the US military,



UK Tweet Promoting US Defense Systems and Military Cooperation

and by extension, these companies bear some responsibility when those weapons are used in disastrous situations.

Earlier this year, Eastern European organizations and media outlets were targeted in a series of suspected Russian cyberattacks to promulgate disinformation. Two months before the Polish election, hackers breached the Polish War Studies Academy and planted false stories in which a Polish general denounced American forces in Poland and claimed the incumbent political party was leading the country to ruin. While short lived, these stories were quickly reposted on social media where they gained more traction and were taken as truth given the source organization.

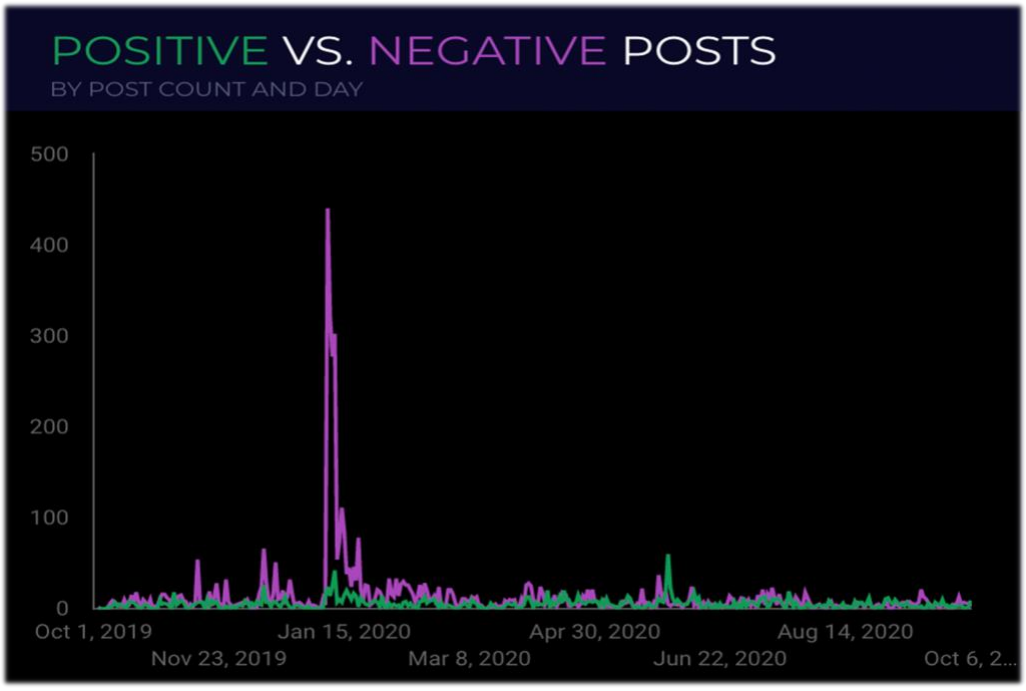
NATO has been a popular target for cyber-enabled IO because of this TTP's ability to leverage the

reputations of trusted media outlets. Whereas RT regularly publishes anti-NATO stories, similar content has begun to appear on pro-Western media sites. In July, Fireeye published a report describing a hacking campaign in which Lithuanian and Polish media organizations were breached and used as platforms for disinformation. News outlets like *The Baltic Course* and *Kas Vyksta Kaune* were specifically targeted and planted with numerous false stories about a planned NATO invasion of Belarus, NATO soldiers spreading coronavirus, and American occupation of Europe.

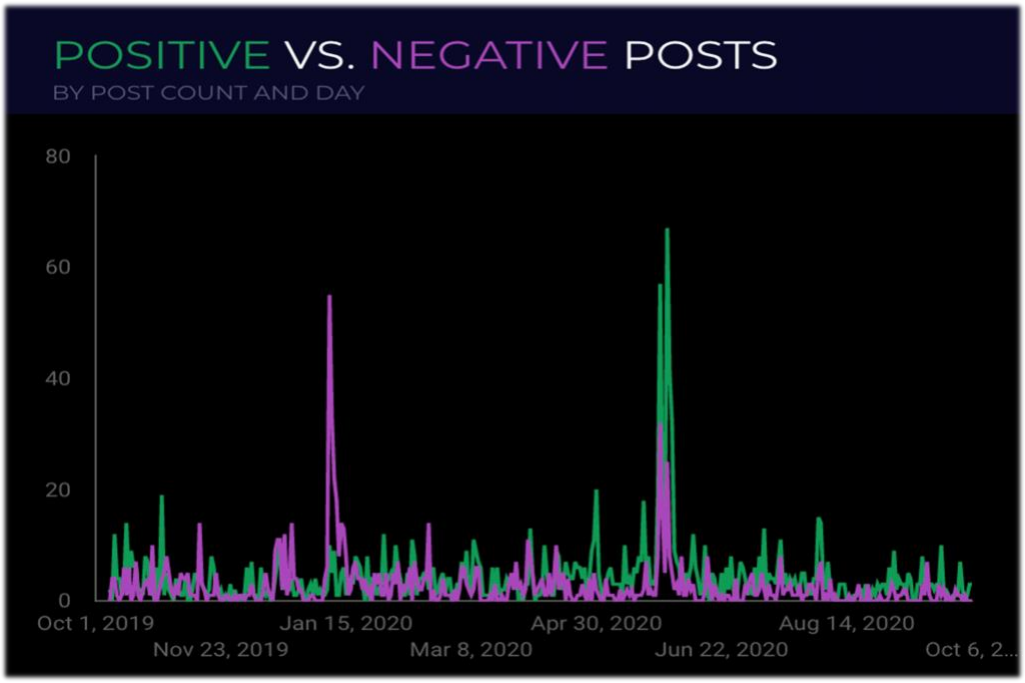
AGENDA-SETTING CAMPAIGNS

Agenda-setting campaigns are an increasingly popular TTP in which marshal the massive capacity of state-run media organizations and coordinate to dominate the global discussion of a specific topic. China and the US have used this TTP in recent months to control narratives surrounding COVID-19. While there is some overlap in terms of post frequency and count, the primary differentiator of this TTP from burst narratives is the longevity of the campaigns. Agenda-setting campaigns sustain the narrative focus and post frequency on a topic for months longer than a burst narrative and permeate the information environment.

Despite aggressive, negative messaging initiatives by Russia and China, the US and UK have conducted an effective campaign to maintain neutral public perceptions of US defense contractors. From October 1, 2019 to October 2020, the US and UK collectively posted 5,815 times about American defense contractors. This contrasts to combined Russian and Chinese posts which stand at over 18,000 in the same time period, with Russia being the primary content producer. Despite being outperformed in raw post count by Russia and China, the US and UK maintained a constant online presence with a particularly positive actor sentiment. These efforts allowed the



The saturation of negative posts by Russia and China is shown here illustrated by more data points in purple throughout the previous year.



US and UK content reflects the opposite of Russia and China: measured coverage of US defense contractors with a moderate tilt toward positive posts. However, US and UK content is negative similarly to Russia and China on the Ukrainian plane crash in January 2020.

US and UK to counter the exceedingly negative content produced by Russia and China.

Sentiment and audience resonance analysis of each actor's messaging reveals that post content can be more important than the raw quantity. US and UK content frames positive content about the defense industrial base in different ways, sometimes touting SpaceX's impressive developments and milestones or mentioning Lockheed's F-35 deployment by allies in joint exercises. The charts below illustrate the disparity in positive to negative content between the two sides, with Russian and Chinese content having a noticeable negative bias that contrasts with generally positive portrayals in US and UK posts. The diversity and frequency of positive content from the US and UK allowed the overall audience sentiment to be minimally impacted by Russian and Chinese negative messaging.

TRENDS FOR THE FUTURE

If there is any single lesson to be gleaned from this report, it is the certainty of disinformation and actor TTPs being employed with greater frequency. US defense contractors are also more important than ever in an era of great power conflict, meaning they will be high value targets for malign IO. The cases described in this report show that defense contractors are frequently the target of online narratives designed to negatively portray the US, whether it be as an incompetent hegemon or a malicious imperial power. As critical structures in the US national security establishment, defense contractors must be aware and prepared to deal with emergent online threats.

The anti-US axis consisting of Russia, China, Iran, North Korea, and Venezuela possesses sophisticated and active online presences that can be marshalled against the US and its allies. Russian and Chinese content reflect a number of common narratives aimed at US information operations; the US will not be able to mount an effective counter messaging operation. Russia alone outperforms the US in raw post count and dominates multiple narratives in US media. IO allies will act as a force multiplier for Russian disinformation, sowing more confusion and falsehoods in an already distorted information environment.

Fortunately, the US and its allies are actively combating negative messaging on the defense industrial base. Predominantly headed by the US and UK, US allies maintain a positive and active presence in the information environment. This advantage will diminish should Russia or China decide to focus more resources to control narratives about the US defense industrial base. The US and its allies need to be prepared for inevitable disinformation campaigns targeting major contractors and be able to quickly respond. The viral nature of online information means that every minute counts in preparing and mounting a counter messaging response.

POLICY RECOMMENDATIONS

A whole of government and interagency solution is required to address the current and growing threat of disinformation against defense contractors. DHS CISA should work with the private sector through a regularly updated platform of detected cybersecurity attacks and suspected disinformation campaigns during their genesis. Active monitoring of the information environment and robust intelligence collection is a critical aspect that will enable any subsequent response to identified operations. Thus, IC elements such as the CIA Open-Source Center and NSA are important stakeholders that will act as a safety net should other IO monitoring methods fail.

The Department of Defense should follow CISA in establishing public-private partnerships to develop a similar database in collaboration with defense contractors to make sure that they do not become targets of IO campaigns. This mandate should be contextualized within physical supply chain and infrastructure resilience, thereby integrating the social supply chain as an important element of defense industrial base security.

Defense contractors themselves have the important role of working with public stakeholders to craft and determine the narratives about their company and the wider industrial base. It is contingent on these contractors to choose how they are portrayed and ensure this portrayal is consistent with American values and beliefs.

GLOSSARY

Actor

A political entity capable of changing the geopolitical landscape, e.g. states, parties, intergovernmental bodies, militias, and foreign terrorist organizations

Account

A unique id within a platform that exists at a distinct URL and which publishes posts.

Brand

Brand is the external facing image of a given account, i.e what the account calls itself without normalization across platforms.

Campaign

One level up in the ontology from narratives, campaigns are the content strategies that an actor has based on their geopolitical objectives. While there might be hundreds of narratives per month, usually, there are only 5-10 campaigns per month. These themes are repeated and used in content generation down the ontology.

Narrative

A narrative is a group of posts whose linked articles have been aggregated according to our story aggregator, i.e. stories are aggregated by linked articles in content and not the content itself. Narratives describe temporally limited events from one or more actors. Each narrative contains multiple posts, but no post can be associated with more than one story.

Online Information Environment

The digital attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization.

Platform

A platform is a social media service or messaging app on which content is published. Platforms available in Open Wolf Totem are Twitter, RSS, YouTube, Telegram, VKontakte, Odnoklassniki, Reddit, Soroush, Aparat, and Instagram. A note on RSS: it is a collection of relevant news feeds, blogs, etc.

Portfolio

Portfolios are the ultimate owner of an account. For government functions, portfolio describes the remit of the portfolio type, e.g. The Ministry of Defense or the Ground Force of the Military, and umbrella brands for media houses, e.g. RT and the Voice of America.

Post

A post refers to specific, distinct online content with an associated unique URL. Posts with the exact same text, posted by the same accounts, but with multiple URLs are multiple pieces of content. Post is the lowest level in our ontology.

Sentiment

Sentiment summarizes on a -1.0 to +1.0 scale how positive or negative is an article, or how negative or positive is an article's portrayal of a given person, place, country, or concept.